VOLUME 4, 2011

ISACA® Journal

Security in a Box

Featured articles:

Information Security Management for Governments

Planning for and Implementing ISO 27001

Measuring and Monitoring Application Security

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

What if you could spend five days...

Exploring the topics most important to you and your enterprise?
Improving your professional skills?
Earning up to 38 continuing professional education (CPE) hours?

You can, at ISACA's Training Week. Reserve your seat today.

8–12 August 2011
Seattle, WA, USA

24–28 October 2011
Baltimore, MD, USA

5–9 December 2011
Scottsdale, AZ, USA

12–16 September 2011
Minneapolis, MN, USA

www.isaca.org/trainingweek-journal

ISACA®
Trust in, and value from, information systems

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

Recognition • Success • Growth

December Exam Date: 10 December 2011
Early Registration Deadline: 17 August 2011

ISACA®
Trust in, and value from, information systems

Volume 4, 2011

ISACA® Journal

Columns

Features

Plus

The *ISACA® Journal* seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The *Journal's* noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.

Read more from these *Journal* authors…

Journal authors are now blogging at *www.isaca.org/journal/blog*. Visit the *ISACA Journal* Author Blog to gain more insight from colleagues and to participate in the growing ISACA community.

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the *Journal*? Additional online-only articles will be available on the first business day of each month in which no *Journal* is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members during their first year of release. Use your unique member login credentials to access them at *www.isaca.org/journalonline*.

Online Features
The following articles will be available to ISACA members online on 1 August 2011.

BMIS—An Introduction to the System Environment
Haris Hamidovic, CIA, ISMS IA, ITIL, IT Project+

Impact of Security Awareness Training Components on Perceived Security Effectiveness
Karen Quagliata, Ph.D., PMP

The Influence of Irrelevant Information on IS Auditor Key Risk Factor Predictions
Daniel D. Selby, Ph.D., CPA

Follow ISACA on Twitter: *http://twitter.com/isacanews*

Join ISACA LinkedIn: ISACA (Official), *http://tinyurl.com/42vbrlz*

Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISACA®
Trust in, and value from, information systems
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org

The Triangulated Pendulum

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

IT leaders were among the first to recognize planning for response to disasters as a business concern, so that the term "disaster recovery planning (DRP)" is usually applied to the recovery of systems, applications and IT infrastructure. Sometime in the 1990s, many people realized that business interruptions happened for reasons other than disasters, and that they affected more than IT, so the term "business continuity management (BCM)" started to be used for the management of the recovery or continuation of business activities in the event of a business disruption.[1] Finally, the term "crisis management planning (CMP)" has been used to refer to preparations for management oversight of the response to the external effects of disruptions to an organization's business affairs.

DATA REPLICATION

There is lively debate about the relationship and relative importance of the three concepts. Broadly speaking, in the 1980s, DRP was the main focus; the 1990s was the time of BCM; and the decade just past saw CMP at the top of the pile.[2] There is no need for me to enter into the discussion because I consider it irrelevant. Organizations should be prepared for unexpected disruptions; no more need be said. Nonetheless, the priority given to one or the other concept has swung like a triangulated pendulum for quite a few years. I see that pendulum swinging once more to the recovery of IT for a number of reasons that may be more substantive than semantic, offering a path to integrating DRP, BCM and CMP.

Not surprising to *ISACA Journal* readers, information systems have massively changed the way organizations conduct business and, thus, the unavailability of those systems would have a massive impact on them. An IT disaster is *ipso facto* a business continuity crisis. As a result, the emphasis in IT has moved in recent years from cure to prevention, i.e., from recovery to resilience. Of course, it was always preferable to prevent disruptions than to react to them. Today, the technical means to continue systems in operation despite disastrous events is now more readily obtainable. The most important technology in this regard is the ability to replicate data from one location to another as they are being written, or at a reasonably short time thereafter.

The cost of data replication is very much an issue, limiting adoption to those organizations with the most money and, then, usually to their most critical information. The interconnectedness of information systems, greatly driven by integrated systems such as enterprise resource planning (ERP) and customer relationship management (CRM), has led to circumstances in which critical data are approaching the totality of organizations' databases. Thus, to replicate just essential data is close to replicating all data.

The cost is justified for businesses with either a high volume of transactions (e.g., orders, trades, shipments) or very limited tolerance for loss of information (e.g., tax filings, research lab findings, medical records). In these instances, the loss of even a relatively small amount[3] of data would have great enough consequences to justify the investment in duplicating data instantly in a remote location so that it would continue to exist if the primary database were destroyed.

> "To replicate just essential data is close to replicating all data."

DATA-DRIVEN CONTINUITY PREPARATION

Data replication is not a new technology, but the breadth of its acceptance is a recent development. What is important is more than just the underlying technology. The vital point from a security perspective is that continuity is being viewed as data-driven. For most of the time that DRP and BCM have been discussed, the primary concern has been the length of time that information systems would be unavailable. It is not that the length of outages is now less

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

of an issue, but that data loss has been recognized as a more serious matter. Business functions are increasingly aware that they can absorb some degree of downtime as long as the information is current (or close) to the point of disruption when systems are recovered. A salutary consequence is that if the investment is made to minimize data loss, the incremental expense to keep application systems running is less of a constraint.

OTHER TECHNOLOGIES

This is made possible to a large extent by virtualization. A few physical servers may be used for purposes other than recovery (e.g., testing, development), with production applications loaded but inactive until they are needed in an emergency, thereby significantly reducing capital expenditure. The greater cost and very much a limiting factor is the cost of an inter-data-center network to transport replicated data. To avoid that expense, most organizations continue to rely on physical and virtual tape backups for less-critical data and applications. The constraint is still the amount of time to restore destroyed data, but the ability to read data from the most advanced tape systems has greatly reduced the amount of downtime. With streaming LTO 5 (or Ultrium) technology, it is possible to transfer a terabyte of data in just over six hours from a single tape.[4, 5] Assuming that multiple drives would be used, the possibility of having data available—if not current to the point of disruption[6]—has made shortened downtime possible. Use of virtual tape libraries (VTL) helps with management of the tapes, but capturing data remotely on tape incurs network cost.

> "The ability to read data from the most advanced tape systems has greatly reduced the amount of downtime."

The pendulum swing toward DRP has been pushed by advances in replication, tape, storage, network and even cloud technology. In what way does this drive the integration of DRP with BCM and CMP? If technology is in place to keep data available and to resume processing quickly, the business impact of an IT failure is reduced to the point that neither a business continuity plan nor a crisis management plan would need to be put into effect. In addition, the Internet and virtual private networks make working remotely a reality, even when there is no disruption.

It is fair to say that this applies only to information-based industries and business functions. People cannot make steel from home.[7] But even steel companies are dependent on their information systems; to a great extent, the failure of centralized IT affects entire organizations more than a disruption at a single factory. In short, BCM and CMP can be dissociated from DRP, but data disruptions ripple through entire organizations.

ENDNOTES

[1] British Standards Institute, BS 25999, *Business continuity management—Part 1: Code of practice*, UK, 2006, p. 1

[2] It was inevitable that the subject would descend into TLAs (three-letter acronyms).

[3] The definition of "relatively small" differs from organization to organization. In some cases, there is zero tolerance for data loss, which significantly raises the cost of replication and limits the location of secondary sites. If the loss of data created or altered in the previous few seconds can be accepted, costs and constraints go down markedly.

[4] Sharwood, Simon; "LTO 5: Fast, vast but still in the past?", TechStorage.com, 30 July 2009, *http://searchstorage.techtarget.com.au/news/2240019182/LTO-5-Fast-vast-but-still-the-past*

[5] Individual vendors of tape systems quote different speeds, some faster, some slower. These should be checked for accuracy. See for instance, IBM (*www-03.ibm.com/systems/storage/tape/ts2250/specifications.html)* or HP *(http://h10010.www1.hp.com/wwpc/us/en/sm/WF06a/12169-304612-3446236-3446236-3446236-4150338.html*).

[6] Thus, actual recovery time includes the time needed to reprocess lost transactions, which for some business functions may not be an issue. Those are the ones for which tape-based data recovery is the preferred alternative.

[7] Originally attributed to Professor Michael Osterholm, University of Minnesota (USA)

Prepare for the **2011** CISA Exams

ORDER NOW—2011 CISA Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Systems Auditor® (CISA®) exam, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses.

www.isaca.org/elearning

www.isaca.org/cisareview

To order CISA review material for the December 2011 exam, visit the ISACA web site at *www.isaca.org/cisabooks* or see pages S1-S8 in this *Journal*.

CISA® Review Manual 2011

ISACA

The *CISA® Review Manual 2011* is a comprehensive reference guide designed to assist individuals in preparing for the CISA exam and individuals who wish to understand the roles and responsibilities of an information systems auditor. The manual has evolved over the past editions and now represents the most current, comprehensive, globally peer-reviewed information systems (IS) audit, assurance, security and control resource available, based on the recently developed 2011 CISA job practice.

The *CISA Review Manual 2011* features a new format. Each of the five chapters has been divided into two sections for focused study. The first section of each chapter contains the definitions and objectives for the five areas, with the corresponding tasks performed by IS auditors and knowledge statements (required to plan, manage and perform IS audits) that are tested on the exam.

Section One is an overview that provides:
- Definitions for the five new areas
- Objectives for each area
- Descriptions of the tasks
- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in Section Two for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section Two consists of reference material and content that supports the knowledge statements. Material included is pertinent for CISA candidates' knowledge and/or understanding when preparing for the CISA certification exam. In addition, the *CISA Review Manual 2011* includes brief chapter summaries focused on the main topics and case studies to assist candidates in understanding current practices. Also included are definitions of terms most commonly found on the exam.

This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

The 2011 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Support
- Protection of Information Assets

CRM-11 English Edition
CRM-11C Chinese Simplified Edition
CRM-11F French Edition
CRM-11I Italian Edition
CRM-11J Japanese Edition
CRM-11S Spanish Edition

CISA® Review Questions, Answers & Explanations Manual 2011

ISACA

The *CISA® Review Questions, Answers & Explanations Manual 2011* consists of 900 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2010* and the 2010 Supplement. Many questions have been revised or completely rewritten to recognize changes based on the new 2011 CISA job practice, and to be more representative of the current CISA exam question format, and/or provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CISA candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISA Review Manual 2011*.

To assist candidates in maximizing study efforts, questions are presented in the following two ways:
- Sorted by job practice area
- Scrambled as a sample 200-question exam

QAE-11 English Edition
QAE-11C Chinese Simplified Edition
QAE-11F French Edition
QAE-11G German Edition
QAE-11I Italian Edition
QAE-11J Japanese Edition
QAE-11S Spanish Edition

CISA® Review Questions, Answers & Explanations Manual 2011 Supplement

ISACA

Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2011 Supplement* is recommended for use when preparing for the 2011 CISA exam. This supplement consists of 100 new sample questions, answers and explanations based on the new 2011 CISA job practice areas, using a process for item development similar to the process for developing actual exam items. The questions are intended to provide CISA candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISA exam.

QAE-11ES English Edition
QAE-11CS Chinese Simplified Edition
QAE-11FS French Edition
QAE-11GS German Edition
QAE-11IS Italian Edition
QAE-11JS Japanese Edition
QAE-11SS Spanish Edition

CISA® Practice Question Database v11

ISACA

The CISA® Practice Question Database v11 combines the *CISA Review Questions, Answers & Explanations Manual 2011* with the CISA Review Questions, Answers & *Explanations Manual 2011 Supplement* into one comprehensive 1,000-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses, and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions. The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:
- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- Microsoft .net Framework 3.5
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

CDB-11 English Edition—CD-ROM
CDB-11W English Edition—Download
CDB-11S Spanish Edition—CD-ROM
CDB-11SW Spanish Edition—Download

CISA Online Review Course

ISACA

A complete web-based exam review course is available at *www.isaca.org/elearning*.

Where Have All the Control Objectives Gone? They Have Picked Them Every One...[1]

Erik Guldentops is an executive professor at the Management School of the University of Antwerp, Belgium, where he lectures on IT security and control, IT governance, and risk management. He worked for many years at SWIFT (Society for Worldwide Interbank Financial Telecommunication), where he held the positions of inspector-general and director of information security and worked with its board and executive management on the subjects of governance, risk, security and control. He held several positions in ISACA and the IT Governance Institute between 1989 and 2007 and helped in the development of COBIT and Val IT. He recently chaired a panel of professors that reviewed the master of IT audit programmes in four universities in The Netherlands.

I still remember the beginning 20 years ago.

It was cold in Paris in November 1991 when ISACA's[2] European Regional Council[3] met. IT audit knowledge was a major theme of the meeting, especially because this group realised that most of the knowledge came from the US. Somewhat desperate for an EU initiative in IT audit research and publications, they 'badgered' me, given my academic contacts, into developing a proposal.

I had been intrigued at the time by EDPAA's *Control Objectives* because, on one hand, it seemed a comprehensive set of the issues of IT audit and control, while, on the other hand, its prescriptive nature and typical audit language made techies and managers apprehensive (to put it mildly). To maintain and enhance its value, it was clear to me that it needed a business foundation and management framework. That became COBIT, and the rest is history…until two weeks ago (at the time of this writing in April 2011).

A brain surge in the middle of the night made me realise—although it was very useful—that we never got it right, in all these years, with the COBIT control objectives (COs). Why? Because of the blurring of objective and action! And it is not the first time that the audit profession has struggled with this. Just think of auditors who often push management to apply specific practices while management has its own ideas about achieving the underlying objectives.

And then, this week, serendipity struck! I got the exposure draft of COBIT 5 for review, and what did I see? The COs are gone! It is good that the development team realised that something needed to be done about that; one can debate, however, about what needed to be done.

This brings me back to the history of COBIT, because we struggled with this for close to 20 years. Maybe we can learn something from our struggles.

The *first* illustration of the issue came with the Peter De Koninck group of experts who began developing the control practices in the second half of the 1990s. They did not explicitly acknowledge the issue of objective vs. action, but, having moved to pure practices, they recognised an underlying need and developed the 'reasons why' to support their practices.

The *second* illustration also came rather early in the COBIT history and relates to the public-sector reaction to COBIT, i.e., that it was not for them. We should have realised that they were partially right, even though the COBIT core development group developed some strong argumentation to the contrary in Washington DC, USA, (of all places) under the guidance of John Lainhart. The action part of the COs might not have always applied to the public sector, but the underlying objective still would have.

A *third* and similar experience occurred with the development of *COBIT Quickstart*. COBIT, having gotten quite some exposure by the late 1990s, had gotten the attention of smaller enterprises and especially consultants and auditors of these entities who were desperately looking for a reference guide, but who justly claimed that COBIT was too much for their purposes. Looking back at the result of that development, especially the second edition of *Quickstart*, I now realise that we evolved the control objectives into pure small-enterprise practices.

The *fourth* lesson (with hindsight) came with COBIT 4. 'Objective' means 'an intention to accomplish', but there is another concept that is between the 'objective' and the 'action', and that is the 'goal'. A 'goal' states the actual achievement of the action and has been a fundamental focus for COBIT 4 in its business, IT and process goal cascade and its development of extensive goal metrics. The highly successful result of that development took our attention away from the still-lingering issue with the control objectives.

My *fifth* example—a strong indication that something was wrong with the COs—was when we recognised the need during COBIT 4 development for the concept of precursors and successors. This concept demonstrates that a CO, now turned into a management practice in one process, will not be successful unless something else has happened in an earlier process (the precursor) and/or until another management practice is applied in a future process (the successor). This shows that control objectives

and processes were not the perfect match that we had thought them to be. We also did not pursue the concept because we could not see how it fit in the framework. This was a warning flag, but got lost in the extensive development projects of COBIT 4.

The *final* piece of the puzzle relates to the ongoing debate of 'best practice' vs. 'good practice' and another concept that I would call 'a necessary and reasonably acceptable practice'. By that, I mean that if there is only *one* good practice or a *necessary but not sufficient* good practice to respond to a control objective, there is a lesser need to make a distinction between objective and action. There are cases like that in the COs, but, I suspect, they comprise a strong minority. One interesting, overlooked example is COBIT's successful process structure, which really is a necessary good practice for efficiently implementing IT goals!

To conclude, there is a need for COs, but they should be *devoid of any implied action*. Maybe calling them control requirements will help. If they were developed like that, they would apply to all enterprises, whatever their industry, sector, size, risk profile or culture.

Such a development initiative would also respond to something that our profession has been lacking: to perform fundamental research into the concepts of IT auditing. I suspect that this could lead us back to the beginning of the COBIT development cycle because control objectives will likely be expressed in the original seven information criteria of COBIT's first edition: efficiency, effectiveness, confidentiality, integrity, availability, compliance and reliability. Testing these principles against later developments such as COSO and ISO 38500, as well as against earlier developments such as Internal Control and Agency Theories, would provide a sound research basis.

Figure 1—A First Cut at Control Requirements for IT

All domains	• Efficiency • Effectiveness • Conformance • …
Governance	• Delegation (including investment to enable IT) • Accountability for that investment towards shareholders • Monitoring and evaluating management • …
Management	• Performance (returning value while managing risk) • Responsibility (for the charge given and resources received) • Directing the enterprise • Aligning (the interests of) different entities • Supervising the enterprise • Measuring results • Continuous improvement • …
Accounting	• Dual control • Segregation of duties • Auditability • …
Security	• Confidentiality • Integrity • Availability • …
Information	• Useful (fit for purpose) • Complete • Accurate • Authentic • Reliable • …
This raises several interesting research questions, such as: • What other domains create control requirements? • How to handle dependencies, e.g., confidentiality as a form of conformance? • Where is the fine line between principle and action, e.g., alignment is a set of management practices to ensure different enterprise entities work together properly, or segregation of duties, which is a management practice for setting up the organisation such that no single individual can perform a sensitive transaction? • What about generally accepted necessary practices that have no (risk-free) alternative such as process-orientation, business/IT alignment or segregation of duties as mentioned above? Do they then become control requirements?	

COs reworked as requirements would fit very well with a new and necessary development in COBIT 5, i.e., the concept of governance enablers—currently defined as frameworks, processes, organisational structures, principles and policies. **Figure 1** provides a 'first cut' of these control requirements.

As a final thought, I plead guilty because I was one of the promoters, in the development of COBIT 4, of the idea to make the COs more (management) action-oriented. It was the right idea, but not at the loss of the essence of the audit and control profession: the true purpose of control. With this year being COBIT's 15th anniversary, it may be good to reflect on past experiences and future objectives.

Over the years, COBIT has secured for ISACA much recognition and honour. Some highlights include:

- A December 2010 report by the IT Policy Compliance Group (ITPCG), titled 'How the Masters of IT Deliver More Value and Less Risk', reveals the 'masters of IT' are using COBIT, IT balanced scorecards and IT portfolio management to improve alignment and deliver more value.
- On 22 August 2010, the Insurance & Capital Market Supervisor in Israel published the final regulations regarding IT governance in institutional bodies that provide insurance and financial services. The regulations declared COBIT an acceptable and recommended control framework for the existence of efficient control and governance mechanisms in IT.
- In September 2009, in a report titled 'Guidance for Best Practices in Information Security and IT Audit', the IT Policy Compliance Group (IT PCG) cites that the best performing organisations uniquely employ COBIT and COSO guidance to inform and guide practices. Practice guidance from COBIT and COSO are cited as 30 times more common among the top performing organisations to inform, guide and adjust information security and audit practices.
- The Government of Alberta, Canada, uses COBIT as the basis for its Information Management and Technology (IMT) Governance Framework to drive a majority of the government-wide IMT policy instruments, such as policy directives, standards and guidelines.
- Text and figures from COBIT 4.1 are used in a white paper titled *U.S. Department of Homeland Security (DHS), Information Technology Governance*, provided by the US Department of Defense.
- The US Postal Service was the first federal agency required to comply with Securities and Exchange Commission rules that enforce the US Sarbanes-Oxley Act. IT governance frameworks, including COBIT, were used to conduct an assessment of IT policies, processes and controls that resulted in a list of gaps that will be addressed as key controls are developed.
- The Information Technology Department of the Government of Kerala, a state in India, issued an order

2011 marks the 15th anniversary of the publication of the first edition of COBIT. ISACA would like to thank all who have participated in COBIT's development over the years, especially those who were instrumental to the first edition:

- Erik Guldentops
- Eddy Schuermans, CISA, CGEIT
- Chris Bagot, CISA
- Gary Austin, CISA, CGEIT, CISSP, PMP
- Rene Barlage
- Rick Beatty
- Henri Beker
- John Beveridge, CISA, CISM, CGEIT
- Peter De Koninck, CISA, CFSA, CIA
- Bart De Schutter
- Balencia Dozier, CISA
- Doris Fong
- Joe Gelinas
- Gary Hardy, CGEIT
- John Hayes
- Greg Hedges, CISM
- A.I. Heijkamp
- Max Huijbers
- Dave Kent, CISA, CGEIT, CGFM
- Tom Kothe, CISA, CPA
- John Lainhart, CISA, CISM, CGEIT, CRISC
- Dan Manson
- Peter Maertens, CA, CFSA, RE
- Akira Matsuo, CISA, CPA
- Bill Pepper
- Robert Roussey, CPA
- Alan Stanley
- Mark Stanley, CISA
- Tjerk Terpstra, CISA
- M.E. Van Biene-Hershey
- Danny Van Riel
- Bram Vandenberg
- Mark Wheeler, CISA, CITP, CPA
- Carla Williams

accepting COBIT as the standard for IT governance as part of its national e-governance plan.

- The Superintendencia Financiera de Colombia, the entity that regulates the banks in Colombia, has adopted and requires the use of COBIT as a reference model for its evaluations, particularly of those entities they supervise, ensuring that these entities, banks and all other financial bodies also use COBIT.
- The Financial Entities General Superintendence in Costa Rica (SUGEF) issued a regulation on information technology (SUGEF 14-09) for institutions under its supervision. Financial institutions must comply with a minimum maturity level of 3 on 17 of the 34 COBIT processes and must have an annual assessment of its IT management framework with an external auditor.
- The National Audit Office of the Lithuanian Republic is using COBIT for auditing the IT activities in the government sector.
- According to the US Office of the Inspector General (OIG), *COBIT Security Baseline* was one of two tool sets for information security programme reviews that were compatible with the National Institute of Standards and Technology (NIST) Framework for performing Federal Information Security Management Act (FISMA) evaluations.

ENDNOTE

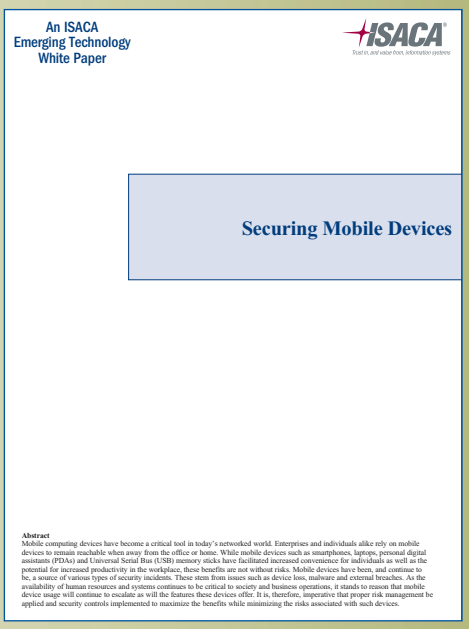
[1] From an ancient Cossack folk song, adapted by Pete Seeger in 1955 into 'Where Have All the Flowers Gone?'

[2] Then, actually still called the EDP Auditors Association. The name changed to ISACA in 1994.

[3] The council was made up of Svein Dovran, Bjorn Hamplund, Henning Walmar, Gary Hardy, Serge Yablonski, Archie Watt and Erik Guldentops.

Download
ISACA'S WHITE PAPERS
for FREE

Get timely, relevant information that you can put to use immediately with ISACA's white papers. The white papers address current business and IT issues, as well as those that will soon impact enterprise operations. White papers are available as complimentary PDF downloads, and no registration is required, so download your copies today and see how your enterprise will benefit from the practical, pragmatic information.



Some of our most recent white papers include:

- *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*
- *Data Leak Prevention*
- *E-Commerce and Consumer Retailing: Risks and Benefits*
- *Electronic Discovery*
- *Securing Mobile Devices*
- *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*
- **And more!**

Don't just take our word for it!

"As information security officer, I found the *Securing Mobile Devices* white paper in particular very useful in highlighting the major vulnerabilities and the business risks associated with mobile device use...a lot of people think purely in terms of technical problems and solutions, so this sort of paper is very helpful in drawing their attention back to business imperatives."

— Rob Dixon, CISA, UK

For a full list of white papers available for FREE download,

www.isaca.org/whitepapers-journal.

ISACA®

Trust in, and value from, information systems

Cloud Computing Risk Assessment
A Case Study

Sailesh Gadia, CISA, ACA, CPA, CIPP, is a director/senior manager at KPMG's advisory practice in Minneapolis, Minnesota, USA. He has an extensive background in designing, implementing and assessing IT controls in various industries and third-party service organizations. Gadia is also an editorial advisor for the monthly *Journal of Accountancy* from the American Institute of Certified Public Accountants (AICPA). His previous *ISACA Journal* article on cloud computing was published in vol. 6, 2009. Gadia can be reached at *sgadia@kpmg.com*.

Cloud computing has come a long way from being a mere buzzword to a meaningful tool with a lot of potential for consumers of technology products and services. The adoption of cloud computing has accelerated in the last few years, and it continues to undergo phenomenal growth.[1]

Just as in the early days of the Internet, there are many unknown variables in cloud computing. Due to its nebulous nature, it is important to understand the risks associated with utilizing cloud computing. It is not just a new technology; it is a different way of doing business.

CASE STUDY

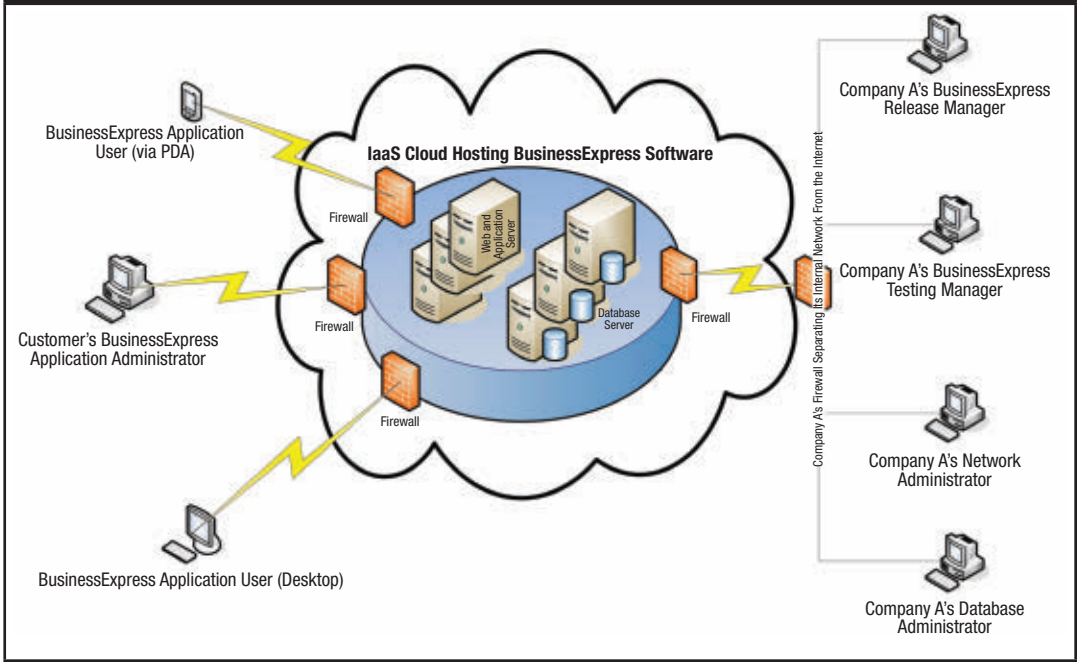
Company A is a start-up that offers business software branded as BusinessExpress. Company A offers BusinessExpress as a Software as a Service (SaaS) solution. The demand for SaaS solutions is expected to grow rapidly. With SaaS, customers enjoy all the benefits of cloud solutions such as not having to host their software in-house[2] (**figure 1**).

Company A's core competency is performing software development, not providing hosting solutions. Infrastructure as a Service (IaaS) cloud service providers (CSPs) specialize in providing hosting solutions. Leveraging an IaaS CSP for hosting has allowed Company A to remain focused on its core competency. There are several other benefits of utilizing an IaaS CSP, such as:[3]

- The ability to offer the software solution on a variety of hardware platforms such as Windows, UNIX and Linux
- Rapid scalability
- Pay-as-you-go capabilities
- Resource availability

Due to the numerous benefits of IaaS, Company A leapt into a cloud computing arrangement. The cloud's economies of scale and flexibility are both a friend and a foe from a security point of view.[4] The chief information officer (CIO) of the company engaged an information systems (IS) auditor to conduct a

Figure 1—Example of an IaaS Cloud Hosting BusinessExpress Software That Is Offered As a SaaS Solution



Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

review and assess the risks of offering a SaaS solution and adopting IaaS cloud computing for this arrangement. The following paragraphs describe the steps followed by the IS auditor to conduct the exercise. This exercise will help the CIO in determining what Company A needs to protect, prioritizing the risks and determining a response.

To conduct a risk-based assessment of the cloud computing environment, there are generic risk frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management—Integrated Framework*. There are also IT domain-specific risk frameworks, practices and process models such as ISO 27001 and IT Infrastructure Library (ITIL). Bottom-up guidance specific to cloud computing also exists from various bodies such as the Cloud Security Alliance (CSA), European Network and Information Security Agency (ENISA), and the US National Institute of Standards and Technology (NIST). The Cloud Controls Matrix released by CSA is designed to provide security principles to guide cloud vendors and assist prospective cloud clients in assessing overall security risks of a CSP. The NIST guidelines on security and privacy in public cloud computing (NIST Special Publication [SP] 800-144), which are currently in draft form, contain the guidelines required to address public cloud security and privacy. The Risk IT: Based on COBIT® framework from ISACA fills the gap between generic risk management frameworks and domain-specific frameworks based on the premise that IT risk is not purely a technical issue.

The IS auditor of Company A chose the Risk IT framework, supplemented with an understanding of the Cloud Controls Matrix, ENISA's cloud computing risk assessment and the NIST guidelines.

Risk IT provides a list of 36 generic high-level risk scenarios, which can be adapted for each organization. Starting with the set of generic risk scenarios helps ensure that the IS auditor does not overlook risks and attains a more comprehensive view of IT risk. Further, Risk IT offers an extensive mapping between the generic risk scenarios and the COBIT control objectives that are customizable for each situation. **Figure 2** illustrates the mapping between the high-level risk scenarios and the corresponding COBIT control objectives created by the IS auditor for the cloud computing arrangement.

Leveraging Risk IT in conjunction with a widely accepted IT governance and controls framework such as COBIT makes the risk identification robust and the risk assessment process

Figure 2—Mapping Between High-level Risk Scenarios and Corresponding COBIT Control Objectives

		COBIT Processes and Corresponding Control Objectives			
Risk IT Reference No.	**High-level Risk Scenarios**	**Plan and Organize (PO)**	**Acquire and Implement (AI)**	**Deliver and Support (DS)**	**Monitor and Evaluate (ME)**
3	Technology selection	PO3.2	AI1.2		
16	Selection/performance of third-party suppliers	PO5.5	AI5.2	DS2.4	
27	Logical attacks		AI2.4	DS5.3, DS5.10	
28	Information media			DS5.11	
31	Data(base) integrity			DS11.6	
32	Logical trespassing			DS5.4, DS5.5	
34	Contractual compliance				ME3.4

Source: ISACA, *The Risk IT Practitioner Guide*, USA, 2009, *www.isaca.org/riskit.pdf*, figure 40

effective and efficient. This leads to a model that is extensible and reusable and that can scale up to IT risks affecting the entire company.

Once the risks and COBIT control objectives were defined, they were used by the IS auditor to develop a risk-based audit program. **Figures 3–10**[5] represent a selection of the audit program for the higher-risk areas in **figure 2**. **Figure 11**

Figure 3—Audit Program: Technology Selection (AI5.2)

Relevant COBIT Control Objective
AI5.2 *Supplier contract management*—Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organizational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.

Audit Procedure
Confirm, through interviews with key staff members, that the policies and standards are in place for establishing contracts with suppliers. Contracts should also include legal, financial, organizational, documentary, performance, security, auditability, intellectual property, responsibility and liability aspects.

Findings
The cloud provider contract does not include certain critical elements to help protect security and privacy requirements. The contract does not include a nondisclosure agreement or a right-to-audit clause. There is no process for the monitoring of potential vendor failure.

An independent auditor's report (e.g., ISAE 3402/SOC 1/SSAE16/SAS 70 report, WebTrust report, SysTrust report) was not reviewed. A review of the report would allow the user organization to understand the controls at the service provider and the nature and extent of controls required to implement.

Figure 4—Audit Program: Selection/Performance of Third-party Suppliers (ME3.4)

Relevant COBIT Control Objective
ME3.4 *Positive assurance of compliance*—Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.

Audit Procedure
Inquire whether procedures are in place to regularly assess levels of compliance with legal and regulatory requirements by independent parties.

Review policies and procedures to ensure that contracts with third-party service providers require regular confirmation of compliance (e.g., receipt of assertions) with applicable laws, regulations and contractual commitments.

Findings
Monitoring of the quality of service (QoS) provided by the CSP needs to be strengthened. Degradation in the QoS may have a significant impact on Company A's ability to meet its obligations to its customers.

In future years, an independent auditor's report (e.g., ISAE 3402/SOC 1/SSAE 16/SAS 70 report, WebTrust report, SysTrust report) would need to be reviewed. A review of the report would help the user organization understand the state of controls at the CSP and whether the user organization needs to add compensating controls.

Figure 5—Audit Program: Logical Attacks (DS5.3)

Relevant COBIT Control Objective
DS5.3 *Identity management*—Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

Audit Procedure
Determine whether access provisioning and authentication control mechanisms are utilized for controlling logical access across all users, system processes and IT resources for in-house and remotely managed users, processes and systems.

Findings
Generic user identifications (IDs) are used to access the virtual servers in the cloud. Multifactor authentication is not utilized for the cloud management console.

Figure 6—Audit Program: Logical Attacks (DS5.10)

Relevant COBIT Control Objective
DS5.10 *Network security*—Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.

Audit Procedure
Inquire whether and confirm that a network security policy (e.g., provided services, allowed traffic, types of connections permitted) has been established and is maintained.

Inquire whether and confirm that procedures and guidelines for administering all critical networking components (e.g., core routers, DMZ, virtual private network [VPN] switches) are established and updated regularly by the key administration personnel and that changes to the documentation are tracked in the document history.

Findings
Application teams currently manage the configuration of the cloud firewall instead of relying on the network engineering team.

Figure 7—Audit Program: Information Media (DS5.11)

Relevant COBIT Control Objective DS5.11 *Exchange of sensitive data*—Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and nonrepudiation of origin.
Audit Procedure Inquire whether and confirm that data transmissions outside the organization require an encrypted format prior to transmission. Inquire whether and confirm that sensitive data processing is controlled through application controls that validate the transaction prior to transmission.
Findings Exchange of sensitive data and administration of cloud instances are done via a regular Internet connection instead of a secure channel such as Secure Sockets Layer (SSL) or Secure Shell (SSH). The organization utilizes an outdated version of Internet Explorer browser software to access and administer the cloud. According to the US Sarbanes-Oxley Act, there need to be proper controls over the initiation, authorization and recording of transactions relevant for financial reporting.

Figure 8—Audit Program: Data(base) Integrity (DS11.6)

Relevant COBIT Control Objective DS11.6 *Security requirements for data management*—Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organization's security policy and regulatory requirements.
Audit Procedure Determine whether a policy has been defined and implemented to protect sensitive data and messages from unauthorized access and incorrect transmission and transport, including, but not limited to, encryption, message authentication codes, hash totals, bonded couriers and tamper-resistant packaging for physical transport.
Findings Personally identifiable information (PII) is stored in clear text at the CSP.

represents a summary of the specific risks and gaps after conducting the audit.

The auditor created a heat map of risks (**figure 12**) that shows the impact/magnitude and likelihood/frequency of key risks relevant to Company A. The combination of higher (negative) impact/magnitude and higher likelihood/frequency of the incident leads to a higher level of business risk. The darker shade indicates unacceptable risk. This level of risk is far beyond Company A's normal risk appetite. (There may be other risks unique to the ultimate end users/customers of Company A, but that is out of scope for this case study.)

Figure 9—Audit Program: Logical Trespassing (DS5.5)

Relevant COBIT Control Objective DS5.5 *Security testing, surveillance and monitoring*—Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.
Audit Procedure Determine whether the IT security management function has been integrated within the organization's project management initiatives to ensure that security is considered in development, design and testing requirements to minimize the risk of new or existing systems introducing security vulnerabilities.
Findings Network diagrams have not been updated to reflect connectivity with the CSP. As a result, the last network penetration testing did not include this as part of the scope.

Figure 10—Audit Program: Contractual Compliance (ME3.4)

Relevant COBIT Control Objective ME3.4 *Positive assurance of compliance*—Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner.
Audit Procedure Inquire whether procedures are in place to regularly assess levels of compliance with legal and regulatory requirements by independent parties. Review policies and procedures to ensure that contracts with third-party service providers require regular confirmation of compliance (e.g., receipt of assertions) with applicable laws, regulations and contractual commitments.
Findings The cloud computing vendor does not have an independent auditor's report (e.g., ISAE 3402/SOC 1/SSAE 16 report).

Due to competing resources, the prioritization of risks related to cloud computing needs to occur, and appropriate action should be taken based on the risk appetite of the company. Appropriate action includes a combination of the following:

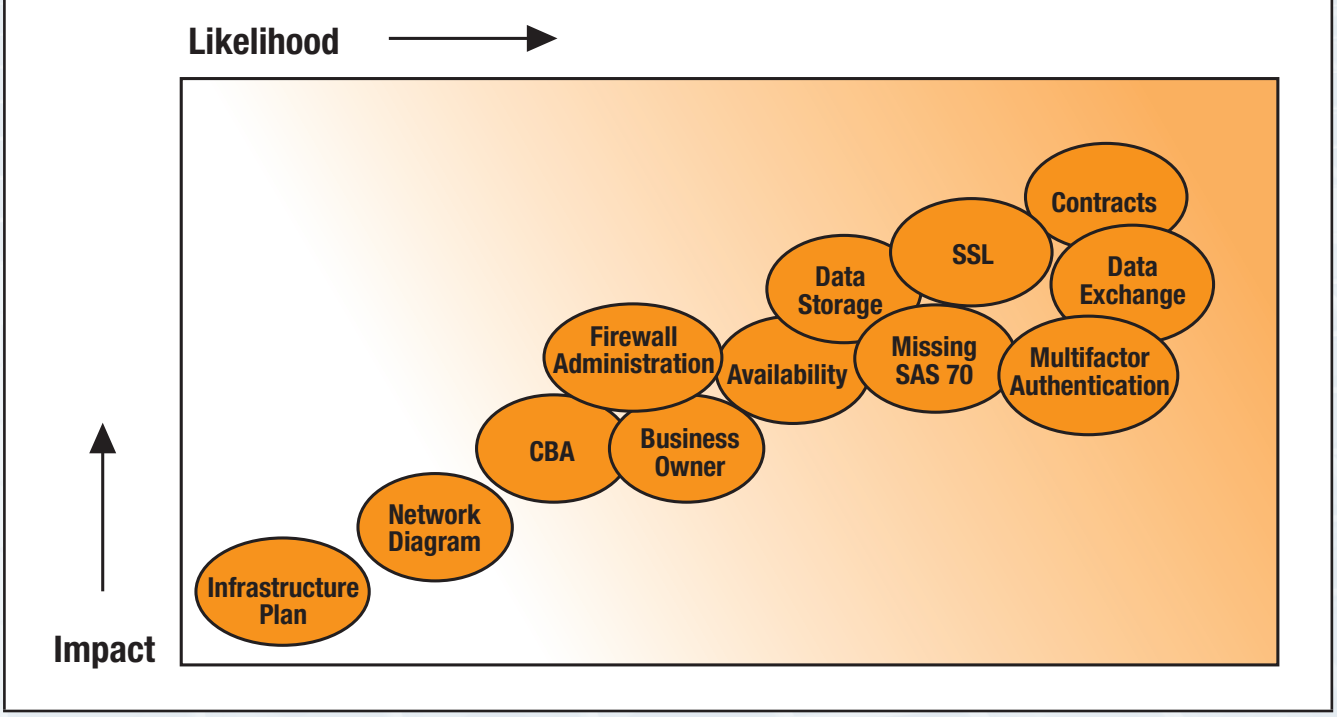
- Implement controls.
- Transfer risk(s).
- Avoid risk(s).
- Accept risk(s).

The audit highlighted that Company A needs to mitigate several risks. However, implementing too many controls may

Figure 11—Summary of Risks and Gaps

Risk IT Reference No.	High-level Risk Scenarios	Specific Risks and Gaps
3	Technology selection	The cloud provider contract does not include certain critical elements to help protect security and privacy requirements and lacks a technology infrastructure plan and a cost/benefit analysis (CBA). An independent auditor's report was not reviewed.
16	Selection/performance of third-party suppliers	Monitoring of the QoS, including availability, needs to be improved. Service level agreements (SLAs) are vague.
27	Logical attacks	The business owner of the IaaS arrangement has not been defined yet. IaaS firewalls are managed by the application team instead of the network administrators. Multifactor authentication is not utilized to administer the cloud.
28	Information media	SSL is not used to exchange sensitive information with the CSP.
31	Data(base) integrity	PII is stored in clear text at the cloud provider.
32	Logical trespassing	Company A's network diagrams have not been updated to reflect the IaaS arrangement.
34	Contractual compliance	The CSP does not go through an independent service auditor's examination.

Figure 12—Heat Map



not be the best risk-mitigation approach because the benefit from implementing controls should outweigh the cost. Other risk-mitigation measures such as transferring, avoiding or accepting the risk are worth considering as well.

Once the company aligns IT risk with the organization's overall business risk and remediates unacceptable security controls, the company is better prepared to harness the power of cloud computing.

CONCLUSION

Businesses are realizing the power of cloud computing, and its use is increasing. This case study represents a one-

time attempt at risk assessment of the cloud computing arrangement. The risk assessment helped uncover some of the key risks, prioritize those risks and formulate a plan of action. Given the evolving nature of risks in cloud computing, no longer can one-time risk assessments suffice. As newer risks emerge, risk assessments need to evolve and the mitigation approach needs to innovate. A risk assessment needs to occur before an enterprise enters into a cloud computing arrangement—to help avoid surprises and minimize the costs of implementing and maintaining controls.

REFERENCES

American Institute of Certified Public Accountants (AICPA), Service Organization Control (SOC) reports, *www.aicpa.org/interestareas/accountingandauditing/resources/soc/pages/sorhome.aspx*

Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," December 2009, USA, *https://cloudsecurityalliance.org/csaguide.pdf*

International Organization for Standardization (ISO), ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2005, *www.iso.org/iso/catalogue_detail?csnumber=42103*

International Federation of Accountants (IFAC), International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, *http://web.ifac.org/download/b014-2010-iaasb-handbook-isae-3402.pdf*

ITGI, *IT Assurance Guide: Using COBIT*, USA, 2007

Office of Government Commerce, IT Infrastructure Library, UK, *www.itil-officialsite.com*

Jansen, Wayne; Timothy Grance; National Institute of Standards and Technology (NIST) Draft Special Publication (SP) 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, USA, 2011, *http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf*

ENDNOTES

[1] Gartner Inc., "Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010," press release, 22 June 2010, *www.gartner.com/it/page.jsp?id=1389313*

[2] Gadia, Sailesh; "Cloud Computing: An Auditor's Perspective," *ISACA Journal*, vol. 6, 2009, *www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/Cloud-Computing-An-Auditor-s-Perspective1.aspx*

[3] Pepitone, Julianne; "Why Attackers Can't Take Down Amazon.com," CNNMoney.com, 9 December 2010, *http://money.cnn.com/2010/12/09/technology/amazon_wikileaks_attack/index.htm*

[4] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, Greece, 2009, *www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment*

[5] IT Governance Institute (ITGI), COBIT® 4.1, USA, 2007

IT Risks—Present and Future

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *ISACA Journal*.

Risk management has become an area of increased focus over the last decade or so. Practically all types of audits begin with a risk assessment and take a risk-based approach. IT managers are equally more focused on IT risk. With the major role that IT risk plays in the current business environment, it is beneficial to understand as much about IT risk as possible. Two recent surveys provide valuable information about IT risks today and in the near future.

AICPA: 2011 TOP 10 TECHNOLOGY INITIATIVES

In 2011, the AICPA conducted its 22nd Top Technology Initiatives (TTI) Survey. Certified Information Technology Professionals (CITPs) and select Certified Public Accountants (CPAs) were asked to rank the technology issues of greatest importance today. The results were divided into those related to public accounting and those related to business and industry. The final composite rankings are included in **figure 1**.

This list provides insight to IT auditors as to some of the major issues most likely to be relevant in today's IT audit environment.

IBM GLOBAL RISK STUDY (2010)

In 2010, IBM conducted a global risk survey of people in various roles to understand how IT managers are working to better understand and mitigate IT risk.

The results show that 66 percent of respondents rate their entity's overall approach to mitigating IT risk as "good to expert." Results also reveal that IT professionals are involved in a number of risk-related issues and feel strongly that they should be even more involved in the future. Current IT risk budgets have not fallen over the last year, but, rather, have remained steady or have increased. Organizations and senior executives recognize the need for and business benefits of risk mitigation. All of these results fall under "good news." The results were also consistent across geographies, industries, size and participant role.

However, there are some areas for improvement and indicators of what the future might hold for IT risks.

Figure 1—AICPA Top 10 Technology Initiatives

Technology Initiative	Public Accounting	Business and Industry
Control and use of mobile devices	1	2
Information security	2	1
Data retention policies and structure	3	3
Remote access	4	5
Staff and management training	5	6
(Business) Process documentation and improvements	6	8
Saving and making money with IT	7	10
Budget processes	9	4
Project management and deployment of new IT	10	9
Technology cost controls	8	-
Key performance indicators	-	7

Present: IT Risk Issues

The survey results included a rating of current IT risk issues. When respondents were asked to identify risk issues of the last year, efforts were focused in a few areas (responding "yes" to the IT risk as a top-of-mind issue):

1. IT security [78%]
2. Hardware and software malfunction [63%]
3. Power failure [50%]
4. Physical security [40%]

Present: IT Risk Maturity

One outcome of the survey was the conclusion that the examination and assessment of an entity's IT risk maturity is foundational to effective risk management. According to the survey, there is a need for an objective assessment of IT risk maturity now. Recommendations included:

- Determine the entity's IT risk maturity with objectivity.
- Institute a cross-functional plan for all risk categories (data, security, recovery and new IT).

- Look at the range of risks and plan for each.
- Search for IT risk champions among senior leaders.
- Articulate the benefits of risk mitigation to all constituents.

Areas the survey identified as major ones for improvement in IT risk maturity include:

1. IT risk planning happens in silos [48%]
2. Creating a formal risk management department [41%]
3. Being more proactive vs. reactive [38%]

Future: Emerging IT Risks

The survey results show several emerging technologies that represent significant IT risks. Those with the most concerns were (rating the IT as "extremely risky/risky"):

1. Social networking tools [64%]
2. Mobile platforms [54%]
3. Cloud computing [42%]

There were some common threads across these risky technologies. One is the security control of the flow of data to and from these technologies. Another was the fact that entities are still struggling with securing their own networks while considering moving to cloud computing; that is, professionals were not sure they were ready internally to extend the IT risks to cloud computing since they were not yet effectively managing IT risks locally. Cutting costs was an attraction for cloud computing in particular, but many consider the risk to be very high.

Social networking and mobile computing concerns were primarily in loss of control of data and threats of unauthorized access to confidential, proprietary data. Overall, social networking and mobile computing were considered very risky.

Future: Shift in Involvement

The survey looked at the current and future involvement of IT managers and professionals in IT risk management. There was a shift predicted three years out—increases in the area of branding (customer service, marketing), business strategy and financials. The decline side of the shift was infrastructure. Perhaps the decline shift is either because infrastructure is being successfully hardened or because entities are moving to cloud computing, Software as a Service (SaaS) and Infrastructure as a Service (IaaS) and, therefore, are able to focus more attention on other areas.

Sixty-five percent of the respondents said that risk mitigation is becoming a more integral part of their job, and 83 percent agree that IT managers should be more involved.

IMPLICATIONS TO IT AUDITORS

First, these surveys provide information to better assess IT risks for any current IT audit activities. In particular, they provide information on emerging issues such as cloud computing and mobile computing. For instance, the IT risk maturity assessment (IBM) would be beneficial information to have for an IT audit. There are areas identified for IT auditors to seek evidence of IT risks and mitigating controls.

The surveys also help focus IT auditors on key issues in performing IT risk assessments. For instance, it is beneficial to compare these two lists and note that mobile computing and information security are prominent on both lists. Risks associated with data are also prominent in both surveys.

The IBM survey also provides forward-looking information to see where IT audits might be moving in the future. Clearly, social networking, mobile computing, cloud computing, SaaS and IaaS (data centers) are areas in which IT auditors will be asked to do more The IBM survey shows the future parties of interest for potential interviews and sources of information for the IT auditor. For instance, IT managers will apparently become even more involved with IT risk assessment and management in the future, at the enterprise level. It is particularly interesting to note that there will be a shift to more involvement by IT managers in financial-related IT risks.

CONCLUSION

Because of the nature of IT, IT auditors have to stay abreast of the ever-changing IT environment. The AICPA TTI and the IBM Global Risk surveys provide valuable information to help keep the IT auditor up to date.

Justin Greis, CISA, CISM, CGEIT, CRISC, CISSP, CIPP, PMP, ITIL, GIAC/GSEC

Justin Greis is a senior manager in the advisory practice of Ernst & Young. He specializes in IT risk and assurance by helping his clients manage risk and improve business performance from their IT investments. Greis has more than 10 years of executive and entrepreneurial leadership experience in IT. He currently also serves as professor of information systems at Indiana University's Kelley School of Business (USA). In 2010, he was selected as one of nine global winners of the Ernst & Young Chairman's Values Award, the firm's highest honor, for his outstanding commitment to the firm's values and its people.

Prior to Ernst & Young, Greis worked as a consultant for Protiviti in Paris and led the technology development of the Eppley Institute for Parks and Public Lands, a nonprofit consulting organization. He was also the founder of an IT consulting and web solutions company, BrainOrbit, which specialized in implementing web-based interactive and training technologies. Greis served as chief executive officer of this organization for four years, before joining the Ernst & Young team.

Greis and his wife, Katharine, founded the "Ernst & Young, James E. Buckman Memorial Fellowship" in memory of Katharine's father. The fellowship is focused on providing post-graduate technology educational opportunities to students in the Kelley School of Business MSIS program at Indiana University. He currently sits on the board of Panna Dolce and resides in Chicago, Illinois, USA.

When not serving his clients, he enjoys playing drums, photography and cooking. He can be reached at *justin.greis@ey.com.*

Q What do you see as the importance and role of values in business?

A Values are the very core of who we are. Without shared values, a business will never be able to articulate its beliefs and demonstrate what makes it different from the next company. We have been witness to countless examples of fraud and inappropriate behavior by business leaders because the ideals for which their companies stood were not truly ingrained into the culture. However, values are just words on a page without the actions to demonstrate that we live what we believe; it is the action and behaviors that strengthen the values for which we stand.

In professional services, much of what we do can be copied or replicated by our competition. We manufacture with our minds, and in the age of information mobility, intellectual capital can leave your company with every employee. So, what makes us as individuals and businesses unique? What differentiates one company from the next? Simply said: It is our values. They create a common bond between our employees and keep our client relationships strong. I believe that the values we instill in our people give us a tangible competitive advantage in the market and make our companies feel like families.

Q What do you see as the biggest risks being addressed by IT governance and risk professionals? How can businesses protect themselves?

A I believe the biggest risk we encounter today has to do with information proliferation and accountability. The features and functionality we build into our advanced information systems to promote integration and interoperability can be turned against us and can introduce risk that must be managed. At E&Y, we call this "the challenge of building trust through information security in a borderless world." Perhaps the most important lesson to keep in mind is that there is no silver bullet, no one tool to manage and control all the IT risks that borderless technologies such as mobile computing, social networking and cloud computing cause. The connectivity and complexity we have built into our systems must be mirrored in the effectiveness of the controls that we design for them. Information security professionals have preached "defense in-depth" for years; it is this concept that should be applied in a company's layered control environment.

But technical controls and automated processes are just one part of the solution; accountability is critical to any controlled environment. It is not sufficient to implement a solution for data protection, application portfolio management or change control, and hope that it works. Functional owners must be empowered to

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

perform their duties, be trained to carry them out and report performance to management, and have the ability to verify the operating effectiveness. Only by creating an environment of accountability can we hope to build a corporate culture that understands the importance and value of doing the right thing. One of the leading indicators that accountability may not exist in a company is the lack of consistent policies, standards and controls. Attempting to instill accountability without such a framework is a tremendous challenge and one many companies struggle with today.

Q How do you see the role of governance of enterprise IT (GEIT) changing in the next five years?

A There are a few areas I see as key to the ever-changing role of GEIT. One of the biggest challenges I have seen has been reporting the right information at the right time to the right executives. Companies have built complex manual processes to generate custom reports so decisions can be made and strategy can be set by executives. Unfortunately, there are many layers of obfuscation that stand between executives and the critical information they need to make wise, well-informed decisions. Think about the game of telephone we used to play as children, and how the message was altered with every person in the link. By the time information reaches executives, it is either incorrect, too late or no longer useful. I have had the good fortune to be a part of programs that streamline the quality and efficiency of the data that get to the right person at the right time. Governance, risk and compliance (GRC) tools, configuration/asset management databases, and project and application portfolio management suites are a step toward elimination of the manual layers that delay bold and decisive action in the governance of IT.

Another key area in which I believe GEIT will change is the concept of IT as a strategic enabler. In some organizations, IT plays more of a support role; it "keeps the lights on" and supports basic business functions. In other organizations, IT is viewed and utilized as a strategic enabler to generate profit or cost savings. The most successful companies I have worked with have embraced technology's role as an enabler rather than the traditional utility model.

Finally, reliance on third parties, vendors and cloud-based models continues to be a major area of focus for IT governance processionals. As the role of the CIO changes from a service provider to a business enabler, we become more reliant on external service providers to introduce new capabilities. Not only are there operational considerations, there is also a whole new world of technology risk and legal considerations introduced by parties that exist outside of our span of influence and sphere of control. Robust vendor management processes can help companies understand the risk, manage the value and optimize the costs associated with outsourced relationships.

Q How did you transition from an entrepreneur to a senior manager in a Big Four firm? Did you find the transition difficult?

A The wonderful part about Ernst & Young is that I never had to transition from being an entrepreneur. We are a company of innovators; the spirit of entrepreneurship exists in every problem we solve and each engagement we execute. When I started BrainOrbit, I built it from scratch and created a place where I would want to work every day. We do the same thing at Ernst & Young; whether at our clients or internally, people with great ideas are a currency valued above all.

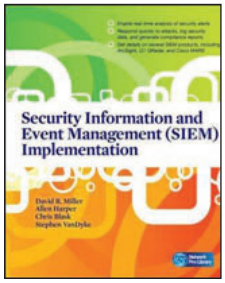
When I started at Ernst & Young, I was worried that the energy and passion I had for new ideas and opportunities would not be valued. But, as I came to know and understand the culture, I found that we are an organization that promotes passion and creativity—and, above all, we reward innovation.

Q What has been your biggest workplace challenge, and how did you face it?

A The biggest challenge for me has been balancing the demands of life on the road with my clients, time in the classroom with my students and my personal life.

I have always loved solving puzzles and figuring out answers to problems; that is why I became a business advisor. My job involves piecing together a jigsaw puzzle and, then, teaching others how to do it all over again. I love spending time with my clients and sharing my experience and knowledge with them. I also spend much of my time on campus at Indiana University teaching in the masters program. But between my two full-time jobs, finding personal time is a challenge. I have an amazingly supportive and inspiring wife and family who are my coaches and mentors. I could not do it without them. However, work-life balance does not just happen; it is planned and must be prioritized as a goal.

Security Information and Event Management Implementation



By David Miller, Allan Sharper, Stephen VanDyke and Chris Blask

Reviewed by Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS, distinguished professor in the law department of the Universidad de los Andes, Colombia. He has been a practitioner and researcher in information and computer security and in computer forensics for more than 15 years in different industries. Cano is a member of ISACA's Publications Subcommittee.

Maintaining a proactive monitoring of a technical and functional infrastructure is a continuing challenge for executives and professionals in information security. Developing the ability to anticipate events and demanding IT insecurity scenarios are permanent tests that question the more elaborate models for the protection of information. In this context, having the security-alert information generated in different parts of our infrastructure and knowing firsthand the security events that occur with the constant interaction of different systems and their participants are urgent needs for proper information security management today.

> "Developing the ability to anticipate events and demanding IT insecurity scenarios are permanent tests that question the more elaborate models for the protection of information."

For this reason, David Miller, Allan Sharper, Chris Blask and Stephen VanDyke presented in this book a strategic and tactical review of deployment systems for monitoring, control and security event correlation, with the aim of generating incident-response capacity and proactive alerts and providing information security managers with a more active posture against the challenges of the complex attacks and failures of the IT available.

Security Information and Event Management Implementation presents analysis of major monitoring solutions, such as event correlation OSSIM, Cisco MARS, ArcSight and Q1 Labs QRadar. For each solution, the book details its technical characteristics and key elements for implementation, with special emphasis on specific considerations to configuration.

Similarly, there is a section in which the authors present elements to develop business intelligence using security information and event management (SIEM) solutions to understand and analyze the changes and evolution of infrastructure and information systems, integrating information from different sources and developing compliance and an effective security posture.

The book can be useful for specialists in information security as well as for information systems auditors, as it allows readers to develop and review policy frameworks to ensure reliable operation with known levels of traceability and control.

IT managers and information security executives facing national and international regulatory and compliance requirements, as well as those who are required to ensure a proactive position to anticipate potential security incidents, can find in this publication SIEM practices with concrete tools to protect enterprise information in an open and interconnected way.

EDITOR'S NOTE

Security Information and Event Management Implementation is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650. ISACA has issued *Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspective*, a white paper available at *www.isaca.org/whitepapers.*

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Hacking Exposed Web Applications:
Web Application Security Secrets and Solutions, 3rd Edition

By Joel Scambray, Vincent Liu and Caleb Sima

Reviewed by Connie Spinelli, CISA, CFE, CIA, CMA, CPA, is a risk management consultant providing governance risk and compliance (GRC), enterprise risk management (ERM) and Sarbanes-Oxley/internal audit program infrastructure solutions and education. Utilizing her experiences and training in the areas of management accounting; internal and external financial, IT and operational audit; and business process risks and controls, Spinelli is in a unique position to strategically work with all members of the C-suite to help them reach their compliance, financial and operational risk management goals. As well as owning her own consulting practice, GRC Solutions LLC, she is a subject matter expert contract writer for Protiviti, a business consulting and internal audit firm.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 3rd Edition is an eye-opening resource for grasping the realities of today's web application security landscape. Accomplished authors Joel Scambray, Vincent Liu and Caleb Sima understand the landscape of the latest web application vulnerabilities as well as the exploitation techniques and tradecrafts that are being deployed against those vulnerabilities.

As businesses push more of their information and commerce to their customers through web applications, the confidentiality and integrity of these transactions is their fundamental, if not mandatory, responsibility. This publication aims to satisfy the needs of those with the need to understand and justify why a control (or corporate expenditure) is necessary. The authors collaborate to provide an easy-to-understand comprehensive blueprint for application developers, security professionals and the auditors charged with living up to this responsibility. Its intended audience is broad, from those with little knowledge or hands-on experience in preventing or detecting web application security to the experienced.

Hacking Exposed Web Applications, begins with a broad overview of web application hacking tools and techniques while showing concrete examples. Each chapter describes one aspect of the attack methodology. Once read as a learning guide or textbook, it should become a desk reference for the business library.

Applicable to all industries, the first section of the book is devoted to describing the basics: web application hacking, infrastructure and application profiling, and web application platforms. The meat of the book is devoted to describing attacks: web authentication and authorization attacks, input injection attacks, web application management attacks, and web client hacks. The second half of the book is devoted to the web application security program and reflects the major components of the full-knowledge methodology: threat modeling, code review and security testing. This third edition embraces the framework concept and integrates the cumulative learning to this point into an "ideal" enterprise web application security program.

Two aspects of the book are of particular note. The book's focus is on identifying, exploiting and mitigating common web application security holes, with an emphasis on server-side flaws, which is expected. However, the book then addresses web-client exploits and vulnerabilities. The authors go beyond the company boundaries to include client exploits: a best-practice exercise for today's security professionals to think beyond their corporate perimeters when brainstorming vulnerabilities and developing their security programs. Second, *Hacking Exposed Web Applications* is written from the perspective of an intruder—another best-practice rule of thumb for those tasked with securing the organization.

The book ends with a comprehensive web application security checklist that summarizes many recommendations and countermeasures made throughout the book, and also serves as a discreet reminder of the many security best practices that should be considered when designing and operating any web application.

The strength of the 450-page book lies in its practicality and usefulness. The authors share a plethora of reference sites and further reading tips, cautions, notes, and best practices. Whether a business leader attempting to understand the threat space for in an enterprise, an engineer tasked with writing code for sites, or a security engineer attempting to identify and mitigate the threats to an application, all readers will benefit from this publication.

EDITOR'S NOTE

Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 3rd Edition is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650.

Information Security Management for Governments

Krishna Raj Kumar, CISA, CISM, is a senior consultant with Barrington Consulting Group based in Halifax, Nova Scotia, Canada. He has worked as an information security manager for more than 15 years within the financial and governmental sectors of the Caribbean, where he last held the position of executive manager, information security in the Government of the Republic of Trinidad and Tobago.

The establishment of common controls and enterprisewide security program development, coordination, implementation and management is the maturation of IS security from a secondary activity to an executive-level operational concern. The key question is: Are not only US government agencies, but also other governments and businesses globally now going to use these new requirements as the impetus of change needed to accelerate the needed improvement in their security readiness and capabilities?[1]

For many governments of developing nations, information security has not yet become an initiative of priority and, as a result, information security may not be supported by the executive in a manner that encourages the measurement and administration of controls that may be necessary to protect the information that is processed, stored and transported by the government's IT systems. The risk associated with not having basic information security controls in place is not always seen as more significant than the initiatives that can gain political mileage. In many cases, the role of information security management (ISM) is often assigned to a single individual, or a very small team, who reports to a senior manager or executive who may have little or no focus on information security.

This article seeks to share a simple model that can be used for ISM in governments. It is meant to assist the IS manager who may be facing challenges in establishing a program that may not be visible or supported by the priorities of the government environment in which the information security manager works.

ISM

ISM should be treated as a specialized function within smaller governments. The information security leader should have direct reporting lines to the head of the government agency responsible for either IT risk management or IT operations. The scope of the information security leader in government needs to be across all of government. An effort to restrict this scope for political or other reasons could compromise the security of information stored, transported and processed by the government. There should be one point of contact for information security at an executive level, and this person must be able to act quickly, at short notice and in a manner that can protect the entire government—within the boundaries of the most senior approval.

The controls recommended in ISO 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, should be implemented in a manner that is applicable to the environment and within budget. A record of all controls that are necessary, but are not achievable within the current budget, should be maintained, and this record should be used to plan each new budget thereafter.

ISM MODEL

Figure 1 depicts an ISM model for smaller governments:

- **Performance measurement**—Before implementing information security controls, it is a good idea to identify the processes that are necessary and to establish a system that will allow the success of the processes to be measured using defined benchmarks against specific control objectives. These processes and methods of measurement are available through COBIT 4.1; however, the value of implementing COBIT can be lost if regular, periodic assessment and measurement are not done.
- **Development**—At least 30 percent of effort should be allocated toward development in each of the seven pillars (discussed in more detail later).
- **Budget**—The information security budget can be continuously justified by asking the executive sponsors pertinent questions such as, "Would it be useful to be able to measure how well the enterprise protects its information?"

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

• **Staffing**—In comparison to other technical departments, information security can function efficiently with a small team of specialists, controlled delegation of responsibilities across other IT departments and outsourcing of specialized activities.

Using ISO 27001 as a guide, the information security department should be built on the following seven pillars of responsibility (**figure 1**).

Information Security Policy

The information security policy should clearly communicate the government's position on the way its computer systems are to be developed, implemented, managed, used and disposed. If previous experience or time is not available, the drafting of the policy can be outsourced and aligned with the vision, environment, culture and IT infrastructure of the government.

A small information security policy review committee should be established that comprises, at a minimum, senior representatives from the most critical departments/ministries (e.g., defense, justice/legal, health, finance). This committee should also include representatives from departments that are critical to the government's economic and political objectives (e.g., energy, industry). Even though it is not necessary for all members of the committee to have a technical background, it is useful if the representatives have a basic understanding of IT and its role in government.

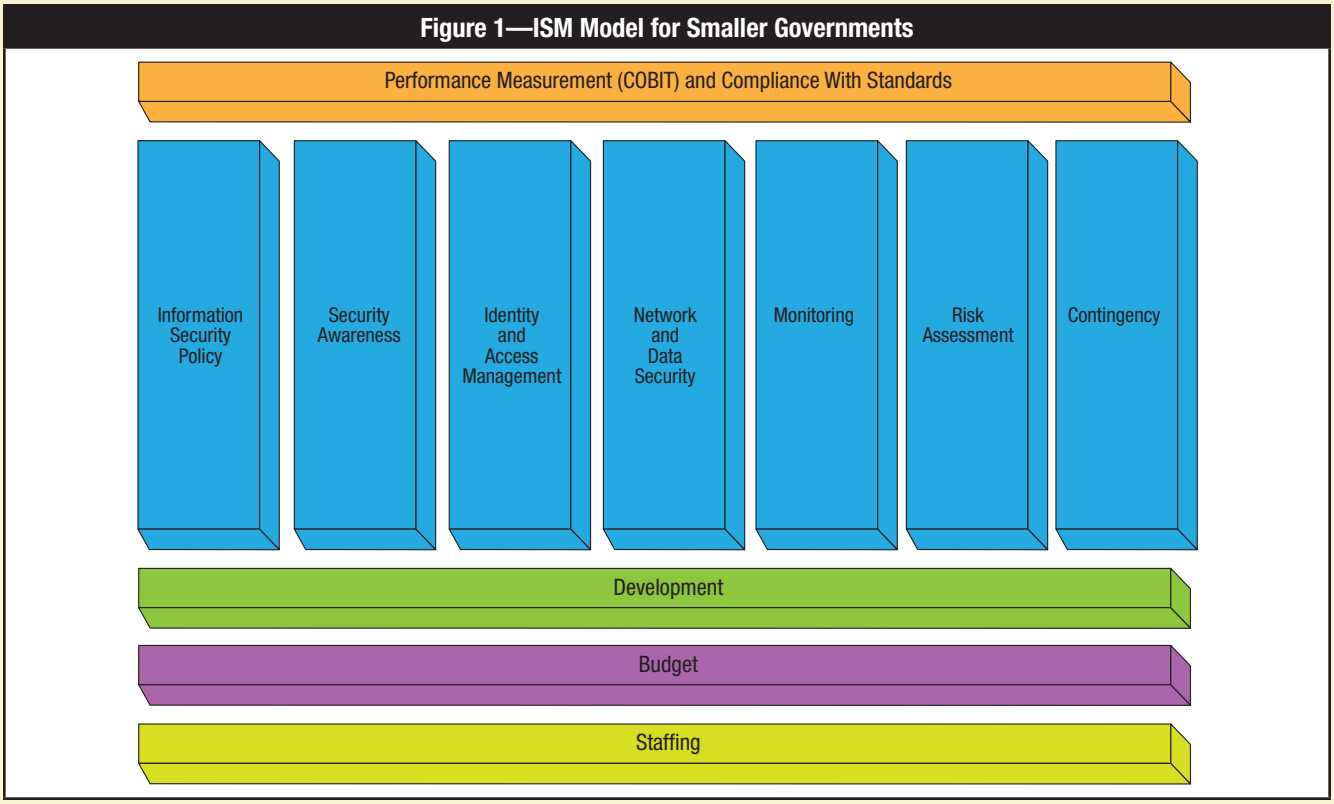
The policy should be approved by the body responsible for government decisions at the highest level (the cabinet, council of ministers or the executive council). It should then be treated as an official government document and be distributed to all government agencies.

Security Awareness

Security awareness is an ongoing process that seeks to ensure that all users are familiar with the information security policies and best practices that govern the use of IT assets.

It is good practice to establish a process whereby new employees are made to attend a security awareness training session as part of their orientation. This can culminate in an online lab session and a quiz to ensure understanding. At the end of the initial training and as part of their annual assessment, all employees should sign a release indicating that they accept and understand the policies.

Figure 1—ISM Model for Smaller Governments



The security awareness program can be split into two specific streams: one geared toward the general user and one that is specialized for technical officers. In the technical officer stream, it is advisable to address the security controls that must be implemented at the system, application, network and database levels. System administrator policies and standards should also be addressed in the technical program.

Due to the number of computer users within most governments, it is often not practical for the information security department to take on the task of conducting the security awareness sessions and may require outsourcing. It is useful to first contract one of these specialized companies to measure the requirements of the training and recommend a customized service based on the size of the network, number of users, categories of users, culture, budget and company information security policies.

> "All access and granting of access should be recorded."

Identity and Access Management (IAM)

A clear hierarchy of access approval should be established with the requisite segregation of duties considered. The information security administrator should not be able to grant access to any system without second approval from the business owner. All access and granting of access should be recorded.

If the budget allows it, a single centralized identity management system (IMS), inclusive of single sign-on (SSO), should be implemented. The key is to be able to view and control a user's access privileges from one place while simplifying the user experience without compromising system security.

For successful IAM:

- All accounts should be uniquely identifiable and assigned to an individual.
- All default accounts should be removed and replaced by uniquely identifiable accounts with the same privileges as the default accounts.
- One account-naming convention should be maintained. For example, avoid using "jbrown" for AS/400 access, "joe_brown" for Windows access and "joe.brown" for UNIX access. An SSO system removes this problem.
- Privileged access activity (e.g., root, admin) should be regularly reviewed, and suspicious events should be investigated.
- Orphan accounts, i.e., accounts that belonged to employees who no longer work for the unit/department, should be closely monitored. These accounts should be disabled and removed as soon as the employee has been terminated.
- Exception reports for multiple password failures should be produced and reviewed daily.
- Audits and "clean-ups" of all user databases should be performed regularly.
- Contractors, auditors and remote system support should be granted only temporary access. If further access is required, the approval process should be followed and recorded.
- Adequate storage space and memory should be available for access logs, and all logs should record who, when, where and what for each instance of access.

Network and Data Security

In the absence of a network security engineer, specific network security processes will be required, and the information security manager will need to ensure that these are assigned to technical resources with the appropriate skills. The information security manager should review daily exception reports because network security administration can be assigned to resources that may not have information security as their daily priority.

All standard network security tools should be assessed and implemented where applicable.

Virtual private networks (VPNs) should be used where applicable, and Internet traffic should be secured and controlled (Secure Sockets Layer [SSL], Secured Hypertext Transmission Protocol [HTTPS], etc.).

The design of the network is extremely important. Critical and vulnerable services should be identified and placed in highly secured network zones. DMZs should be implemented and used to separate critical services from lower-risk services.

Network policies should be reviewed regularly and implemented at all times. It is recommended to have a centralized network policy management system from which policy modules can be applied to network elements.

Network policies should mandate that all network clients (personal computers [PCs], laptops, etc.) have a defined, minimum set of security controls in place before they are authenticated to the network. For example, all laptops should have the latest antimalware software updates installed before access to network services is granted.

Operating system (OS) patch levels should be applied across the organization after being tested in an isolated environment. This includes all security updates that may have been implemented by the OS vendors.

Network access logs should be reviewed daily, and all suspicious activity should be reported according to a defined escalation procedure and addressed as quickly as possible.

Monitoring

The assumption that the network is not under threat is normally a perception created by a lack of adequate monitoring. The information security manager within the government must ensure that there are ongoing and measurable information security incident monitoring processes in place at both the internal and national level.

The key watch words of monitoring are: who, when, where and what.

At an internal level, incident reporting resources and tools should be deployed at all times. Surveillance of all networks and data repositories is critical. Automated alerting mechanisms and escalation procedures should be designed and implemented. Exception reports should be reviewed daily. Extra storage for log files should be identified, and all access logging should be activated. A corporate logging strategy should be implemented that includes, but is not limited to, log rotation strategy, archiving and remote journaling.

Internal information security monitoring can be the responsibility of the network group or the help desk, and most of it can be automated.

At the external or national level, the information security manager within the government should be actively involved in running a national computer security incident response team (CSIRT).

Assistance in setting up a national CSIRT is readily available from the Inter-American Committee Against Terrorism (CICTE).[2] The national CSIRT team should comprise members from a cross-section of the society. Education, military, critical industry and the private business sector should all be actively involved. The national CSIRT should be closely linked with other regional CSIRTs and should have a direct escalation path to the government executive responsible for national security.

Risk Assessment

In the case of information security, risk assessment consists of a number of techniques used to identify and report weaknesses and to recommend mitigating controls. This is an ongoing process of checking for existing risks and recommending mitigation.

A cycle to identify information security risks should be established. This includes identification of both IT system and process vulnerabilities. For example, is it possible for the network administrator to create user accounts anonymously without trace or approval? These tests should be conducted by independent, third-party security specialists. It is best practice to alternate among the contracted third parties on an annual basis, thus ensuring that any biases are avoided and a wider spread of results is achieved.

The resulting threat analysis reports should be used to determine levels of risk and to apply priorities in budgets and remedial activity. Generally, information security risk (R) can be approximated by determining the measurement of the probability (P) of an event occurring, the value (V) of the asset that may be at risk and the threat (T) itself. In mathematical terms, the rough equation is: R = PVT.

All recommended mitigation should be submitted to senior management. The enterprise may be willing to accept the risk regardless of the cost of mitigation because the risk may have a low impact or its likelihood may be low. It is up to the senior management team to determine the enterprise risk tolerance level and to inform the information security manager as to whether the recommended mitigation should be implemented.

> “It is best practice to alternate among the contracted third parties on an annual basis.”

The cost of implementing the countermeasure equals the cost of the asset multiplied by the value percentage of the overall infrastructure, which is then multiplied by the annualized rate of occurrence (ARO).

The exercise of achieving accurate calculations of risk in this manner can be time-consuming and highly subjective. For smaller information security departments, it is probably more worthwhile to outsource the threat analysis and address the identified weaknesses, in order of criticality, as soon as possible. For the organization that determines that it is worthwhile to measure risk, *The Risk IT Practitioner Guide* from ISACA and ISO 27005:2008, *Information technology—Security techniques—Information security risk management*, can be used for guidance.

Contingency

Contingency planning would normally fall under the scope of the risk management department; however, in smaller governments, the responsibility often ends up with the information security department for various reasons.

In this case, contingency planning involves business continuity planning (BCP) and disaster recovery planning (DRP) as it relates to IT infrastructural design and IT business support processes. The objective is to ensure minimal service disruption and the reestablishment of business services in the shortest possible time after an unforeseen event or a disaster occurs.

The contingency planning process does not refer only to backup and restoration; it also includes the following steps:

- Develop a contingency planning policy statement.
- Conduct a business impact analysis (BIA).
- Identify preventive controls.
- Develop recovery strategies.
- Develop an IT contingency plan (including a sequence of recovery).
- Plan testing, training and exercises.
- Plan maintenance.

The contingency strategy must be developed in cooperation with other functional and resource managers associated with the system or the business processes supported by the system. All major applications and general support systems must have a contingency plan.[3]

From implementation of storage access networks (SANs) and data restoration to the development of the emergency contact list for the server room, the IT contingency coordinator (in the case of smaller governments, the information security manager) must be able to understand and coordinate the processes that are necessary. A great place to start is with the identification of the critical business services and their supporting infrastructure, i.e., the services that, if unavailable, would disable the ability to achieve organizational goals and would result in loss of revenue, reputation and legal compliance.

It is recommended that the information security manager become familiar with the contingency planning guide for IT systems published by the US National Institute of Standards and Technology in 2002.

CONCLUSION

In governments that place less importance on the needs and risks associated with the security of the information that is stored, transported and processed by their IT systems, the information security manager may find it easier to establish a successful and sustainable ISM function by implementing a model that includes information security policy, information security awareness, IAM, network and data security, information security monitoring, and risk assessment and contingency as functional pillars. These functions should be supported by continuous measurement and compliance, development, and appropriate budgeting and staffing.

ENDNOTES

[1] Roth, Jeff; "Evolution of Federal Cybersecurity—From Individual Controls to Systems of Control," JournalOnline, *ISACA Journal*, vol. 5, 2010, *www.isaca.org/journalonline*

[2] In 2004, in recognition of the emerging threats to the Internet and related computer systems, the Organization of American States (OAS) General Assembly adopted a "comprehensive inter-American strategy to combat threats to cybersecurity." The strategy calls for all member states to establish or identify national "alert, watch and warning" groups known as computer security incident response teams (CSIRTs) and to take the necessary measures to prevent cyberthreats, prosecute cybercrimes and promote a culture of awareness in their countries. To help implement these three pillars of strategy, three OAS committees joined forces—the Inter-American Committee Against Terrorism (CICTE), the group of governmental experts on cybercrime of the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA), and the Inter-American Telecommunications Commission (CITEL).

[3] National Institute of Standards and Technology (NIST), *Contingency Planning Guide for Information Technology Systems*, USA, 2002, *www.itl.nist.gov/lab/bulletns/bltnjun02.htm*

Feature

Planning for and Implementing ISO 27001

Charu Pelnekar, CISA, CISM, ACA, AICWA, BCOM, CISSP, CPA, MCSE, QSA, is a director with Professional Consultant, a consulting firm. He has skills in business and technology consulting, as well as experience with audits and risk management, process reengineering, and business management. Since 1993, he has worked in an advisory role with national and international corporations across various industries. He served as vice president, in 2007–2008, and as membership director, in 2006–2007, of the ISACA Austin (Texas, USA) Chapter. He can be contacted at *charpeln@hotmail.com.*

ISO/IEC 27001:2005 *Information Technology—Security techniques—Information security management systems—Requirements* is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).[1, 2] The potential benefits[3, 4] of implementing ISO 27001 and obtaining certification are numerous. Implementing ISO 27001 can enable enterprises to benchmark against competitors and to provide relevant information about IT security to vendors and customers, and it can enable management to demonstrate due diligence. It can foster efficient security cost management, compliance with laws and regulations, and a comfortable level of interoperability due to a common set of guidelines followed by the partner organization. It can improve IT information security system quality assurance (QA) and increase security awareness among employees, customers, vendors, etc., and it can increase IT and business alignment. It provides a process framework for IT security implementation and can also assist in determining the status of information security and the degree of compliance with security policies, directives and standards.

The goal of this article is to provide guidance on the planning and decision-making processes associated with ISO 27001 implementation, including associated costs, project length and implementation steps.

COSTS OF IMPLEMENTATION

Before implementing ISO 27001, one needs to consider the costs and project length, which are further influenced by the detailed understanding of the implementation phases. Any cost is painful in tough economic times. In today's cloud computing environment, organizations that want to reduce costs without compromising information security are looking at ISO 27001 certification as a promising means to provide knowledge about their IT security.

Implementation costs are driven by the perception of risk and how much risk an organization is prepared to accept. Four costs need to be considered when implementing this type of project:

1. **Internal resources**—The system covers a wide range of business functions including management, human resources (HR), IT, facilities and security. These resources will be required during the implementation of the ISMS.
2. **External resources**—Experienced consultants will save a huge amount of time and cost. They will also prove useful during internal audits and ensure a smooth transition toward certification.
3. **Certification**—Only a few approved certification agencies currently assess companies against ISO 27001, but fees are not much more than against other standards.
4. **Implementation**—These costs depend largely on the health of IT within the organization. If, as a result of a risk assessment or audit, a gap appears, then implementation costs are bound to go up based on the solution implemented.[5]

On average, implementation of a system such as this can take four to nine months and depends largely on the standard of conduct and quality and management support (tone at the top[6]), the size and nature of the organization, the health/maturity of IT within the organization, and existing documentation.

ISO 27001 requires a company to establish, implement and maintain a continuous improvement approach to manage its ISMS. As with any other ISO compliance, ISO 27001 follows the plan-do-check-act (PDCA) cycle, as shown in **figure 1**.

The cost factors mentioned earlier are directly impacted by the inventory of IT initiatives within the organization. Organizations with COBIT framework, Statement on Auditing Standards (SAS). No. 70 Type I and Type II, Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), or US Sarbanes-Oxley Act capabilities in place provide a ready inventory of set policies

Figure 1—PDCA Cycle and Respective Implementation Phases

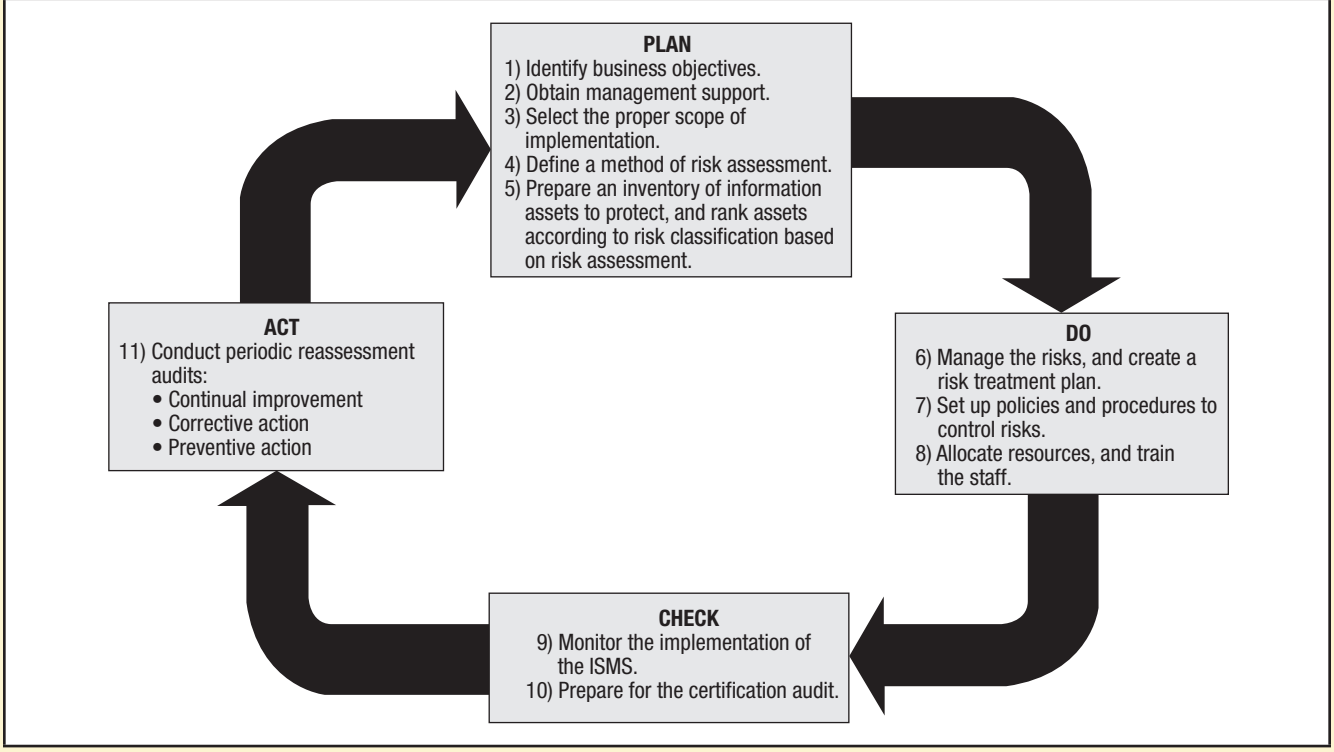


Figure 2—Time and Cost Savings on Respective PDCA Phases Associated With the IT Initiative

IT Initiative	Ready Information Inventory	Time and Cost Savings on the Following PDCA Phases
COBIT	Policies, procedures, risk assessment, control objectives and controls	Phase 2—Obtain management support. Phase 3—Select the proper scope of implementation. Phase 4—Define a method of risk assessment. Phase 5—Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment. Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks. Phase 8—Allocate resources, and train the staff.
SAS 70 Type I and Type II	Policies, procedures, risk control objectives and controls	Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks.
NIST	Risk assessment, detailed control objectives and controls	Phase 2—Obtain management support. Phase 3—Select the proper scope of implementation. Phase 4—Define a method of risk assessment. Phase 6—Manage the risks, and create a risk treatment plan.
PCI DSS	Detailed control within the PCI DSS framework	Phase 6—Manage the risks, and create a risk treatment plan.

and procedures, risk assessments, control objectives, and operational controls that can often significantly reduce the time and expense needed to complete the project. Refer to **figure 2** to understand the time and cost savings on respective PDCA phases associated with different IT efforts.

In addition to the previously mentioned cost savings, the organization that wants to have a step-by-step approach to ISO compliance can adopt a corporate scheme, which envisages that the scope of compliance can be restricted to a specific division, business unit, and type of service or physical location. The adoption of a corporate scheme will save time and allow the organization to realize the benefit of ISO 27001 certification. In addition, once successful compliance has been achieved for a limited, but relevant, scope, the corporate scheme can be expanded to other divisions or locations.

ISMS—PLANNING FOR ISO

ISO/IEC 27001 and its supporting document, ISO/IEC 27002 (ISO/IEC 17799), detail 133 security measures, which are organized into 11 sections and 39 control objectives. These sections specify the best practices for:

- Business continuity planning
- System access control
- System acquisition, development and maintenance
- Physical and environmental security
- Compliance
- Information security incident management
- Personnel security
- Security organization
- Communication and operations management
- Asset classification and control
- Security policies

The ISMS may be certified as compliant with ISO/IEC 27001 by a number of accredited registrars worldwide. The ISO/IEC 27001 certification, like other ISO management system certifications, usually involves a three-stage audit process:

- **Stage 1**—Informal review of the ISMS that includes checking the existence and completeness of key documents such as the:
  - Organization's security policy
  - Risk treatment plan (RTP)
  - Statement of applicability (SOA)
- **Stage 2**—Independent tests of the ISMS against the requirements specified in ISO/IEC 27001. Certification audits are usually conducted by ISO/IEC 27001 lead auditors.

- **Stage 3**—Follow-up reviews or periodic audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic reassessment audits to confirm that the ISMS continues to operate as specified and intended.

Independent assessment necessarily brings some rigor and formality to the implementation process, and it must be approved by management. ISO/IEC 27001 certification should help assure most business partners of the organization's status regarding information security without the business partners having to conduct their own security reviews.

Planning

As in all compliance and certification initiatives, consideration of the organization's size, the nature of its business, the maturity of the process in implementing ISO 27001 and commitment of senior management are essential. The most important departments and activities that will be vital to the success of the project include:

- **Internal audit**—During the initial planning phase, the input from internal audit will be useful in developing an implementation strategy, and early involvement of internal auditors will be useful during the later stages of certification that require review by management.
- **IT**—The IT department will have to dedicate resources and time to the activities associated with the ISO 27001 initiatives. An inventory of existing IT compliance initiatives, procedures and policies, and the maturity of existing IT processes and controls will be useful to gain an understanding of how the existing processes align with ISO 27001 requirements.

Although implementation of policies and procedures is largely perceived as an IT activity, other departments play an important role in the implementation. For example, facilities management is largely responsible for physical security and access controls.

Decision Making

The decision of when and how to implement the standard may be influenced by a number of factors, including:

- Business objectives and priorities
- Existing IT maturity levels
- User acceptability and awareness
- Internal audit capability
- Contractual obligations
- Customer requirements
- The enterprise's ability to adapt to change
- Adherence to internal processes
- Existing compliance efforts and legal requirements
- Existing training programs

IMPLEMENTATION PHASES

Various IT initiatives that can save time and cost on implementation phases are illustrated in **figure 2**. As explained earlier, an organization also needs to have the detailed understanding of PDCA implementation phases to manage the costs of the project. The cycle of PDCA is consistent with all auditable international standards: ISO 18001, 9001 and 14001. ISO/IEC 27001:2005 dictates the following PDCA steps for an organization to follow:

- Define an ISMS policy.
- Define the scope of the ISMS.
- Perform a security risk assessment.
- Manage the identified risk.
- Select controls to be implemented and applied.
- Prepare an SOA.

These suggested PDCA steps are further simplified and mapped (**figures 1, 3** and **4**) to the implementation phases developed for easy understanding and implementation—with the end objective of time and cost savings in mind. The following steps take into account the IT maturity within the organization and the review/registration process (see **figure 4** for the details of review and registration steps).

Phase 1—Identify Business Objectives

Stakeholders must buy in; identifying and prioritizing objectives is the step that will gain management support. Primary objectives can be derived from the company's mission, strategic plan and IT goals. The objectives can be:

- Increased marketing potential
- Assurance to the business partners of the organization's status with respect to information security
- Assurance to customers and partners about the organization's commitment to information security, privacy and data protection
- Increased revenue and profitability by providing the highest level of security for customers' sensitive data
- Identification of information assets and effective risk assessments
- Preservation of the organization's reputation and standing among industry leaders
- Compliance with industry regulations

Figure 3—Mapping ISO/IEC 27001 Suggested Steps to Implementation Phases

ISO/IEC 27001:2005 Suggested Steps	Implementation Phases
Define an ISMS policy.	Phase 1—Identify business objectives. Phase 2—Obtain management support.
Define the scope of the ISMS.	Phase 3—Select the proper scope of implementation.
Perform a security risk assessment.	Phase 4—Define a method of risk assessment.
Manage the identified risk.	Phase 5—Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment.
Select controls to be implemented and applied.	Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks. Phase 8—Allocate resources, and train the staff.
Prepare an SOA.	

Figure 4—Mapping Implementation Phases to Review and Registration Steps

Review and Registration Steps	Implementation Phases
Management review and internal audit	Phase 9—Monitor the implementation of the ISMS.
Registration and certification	Phase 10—Prepare for the certification audit.
ISMS improvement	Phase 11—Conduct periodic reassessment audits: • Continual improvement • Corrective action • Preventive action

Phase 2—Obtain Management Support

Management must make a commitment to the establishment, planning, implementation, operation, monitoring, review, maintenance and improvement of the ISMS. Commitment must include activities such as ensuring that the proper resources are available to work on the ISMS and that all employees affected by the ISMS have the proper training, awareness and competency. The following activities/initiatives show management support:

- An information security policy
- Information security objectives and plans
- Roles and responsibilities for information security or a segregation of duties (SoD) matrix that shows the list of the roles related to information security
- An announcement or communication to the organization about the importance of adhering to the information security policy
- Sufficient resources to manage, develop, maintain and implement the ISMS
- Determination of the acceptable level of risk
- Management reviews of the ISMS at planned intervals
- Assurance that personnel affected by the ISMS are provided with training
- Appointment of competent people for the roles and responsibilities that they are assigned to fulfill

Phase 3—Select the Proper Scope of Implementation

ISO 27001 states that any scope of implementation may cover all or part of an organization. According to section B.2.3, Scope of the ISMS, only the processes, business units, and external vendors or contractors falling within the scope of implementation must be specified for certification to occur.

The standard also requires companies to list any scope exclusions and the reasons why they were excluded. Identifying the scope of implementation can save the organization time and money. The following points should be considered:

- The selected scope helps to achieve the identified business objectives.
- The organization's overall scale of operations is an integral parameter needed to determine the compliance process's complexity level.
- To find out the appropriate scale of operations, organizations need to consider the number of employees, business processes, work locations, and products or services offered.
- What areas, locations, assets and technologies of the organization will be controlled by the ISMS?
- Will suppliers be required to abide by the ISMS?
- Are there dependencies on other organizations? Should they be considered?
- Any regulatory or legislative standards that apply to the areas covered by the ISMS should be identified. Such standards may come from the industry in which the organization works; from state, local or federal governments; or from international regulatory bodies.

The scope should be kept manageable, and it may be advisable to include only parts of the organization, such as a logical or physical grouping within the organization.

Phase 4—Define a Method of Risk Assessment

To meet the requirements of ISO/IEC 27001, companies need to define and document a method of risk assessment. The ISO/IEC 27001 standard does not specify the risk assessment method to be used. The following points should be considered:

- The method to be used to assess the risk to identified information assets
- Which risks are intolerable and, therefore, need to be mitigated
- Managing the residual risks through carefully considered policies, procedures and controls

Choosing a risk assessment method is one of the most important parts of establishing the ISMS. Use of the following will be helpful:

- NIST Special Publication (SP) 800-30 *Risk Management Guide for Information Technology Systems*
- Sarbanes-Oxley IT risk assessment
- Asset classification and data classification documents (determined by the organization)

ISO 27001 needs risk evaluations based on levels of confidentiality, integrity and availability (CIA):

- **Confidentiality**—Clause 3.3: Ensuring that information is accessible only to those authorized to have access
- **Integrity**—Clause 3.8: Safeguarding the accuracy and completeness of information and processing methods
- **Availability**—Clause 3.9: Ensuring that authorized users have access to information and associated assets when required

Phase 5—Prepare an Inventory of Information Assets to Protect, and Rank Assets According to Risk Classification Based on Risk Assessment

The company needs to create a list of information assets to be protected. The risk associated with assets, along with the owners, location, criticality and replacement value of assets, should be identified. Information regarding the grouping of assets, data classification documents and assets inventory documents will be useful. Following are suggested steps:

- For assets, identify the CIA impact levels: high, medium and low.
- Identify risks, and classify them according to their severity and vulnerability.
- After identifying the risks and the levels of CIA, assign values to the risks.
- Based on risk values, determine whether the risk is tolerable and whether to implement a control to eliminate or reduce the risk. The risk assessment methodology will guide in establishing risk levels for assets.

Once the assessment is completed, the information assets that have intolerable risk and, therefore, require controls will be identified. At that time, a document (sometimes referred to as a risk assessment report) that indicates the risk value for each asset is created.

Phase 6—Manage the Risks, and Create a Risk Treatment Plan

To control the impact associated with risk, the organization must accept, avoid, transfer or reduce the risk to an acceptable level using risk mitigating controls. The next stage is performing the gap analysis with the controls provided in the standard (refer to Annex A of ISO/IEC 27001 or to ISO/IEC 27002) to create an RTP and an SOA. It is important to obtain management approval of the proposed residual risks.

The RTP (**figure 5**) provides:

- Acceptable risk treatment (accept, transfer, reduce, avoid)
- Identification of operational controls and additional proposed controls, with the help of gap analysis
- A proposed control implementation schedule

Figure 5—Risk Treatment Plan

Risk	Explanations of Risk Treatment Categories			
	Reduce	Avoid	Accept	Transfer
Information security risk	Reduce or mitigate the risk; refer to the 133 controls to identify and implement suitable information security controls or the other initiatives in the organization, e.g., ITIL, COBIT.	Avoid the situation that creates the risk by proactive planning, redesigning or reengineering.	Management should acknowledge the residual risk if there is no cost-effective solution.	Is it possible to transfer some or all of the risk to a third party (insurer)?
Risk and Risk Treatment Example With Applicable Controls				
Inappropriately configured firewall rule sets increasing the risk of unauthorized access to critical and/or privileged network resources	Management performs and reviews vulnerability assessments on an annual basis.	Management has defined perimeter security controls, including firewalls and intrusion detection systems.		

Figure 6—Example SOA for Applicable Controls

Control Objective	Control From Annex A of ISO/IEC 270001	Adopted or Not Adopted	Justification	Organization Procedures and Reference
Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	10.5.1 Information Backup	Adopted	Management has implemented a strategy for cyclical backup of data and programs.	XXX—Information security policy XXX—Information backup and media protection procedure

Figure 7—Referenced Policies and Procedures to Control Risks Example						
ISO 27001:2005 Controls						
Clause	Section	Control/Control Objective	Existing Controls	Excluded Controls	Justification	Reference Policies and Procedures
Information systems acquisition, development and maintenance	12.4	Security of system files	Yes		Best practices	Systems acquisition/ development policy
	12.4.1	Control of operational software				
	12.4.2	Protection of system test data				

The SOA documents the control objectives (**figure 6**), the controls selected from Annex A, and the justification for adopting or not adopting the control.

Phase 7—Set Up Policies and Procedures to Control Risks
For the controls adopted, as shown in the SOA, the organization will need statements of policy or a detailed procedure and responsibility document (**figure 7**) to identify user roles for consistent and effective implementation of policies and procedures.

Documentation of policies and procedures is a requirement of ISO/IEC 27001. The list of applicable policies and procedures depends on the organization's structure, locations and assets.

Phase 8—Allocate Resources, and Train the Staff
The ISMS process highlights one of the important commitments for management: sufficient resources to manage, develop, maintain and implement the ISMS. It is essential to document the training for audit.

Phase 9—Monitor the Implementation of the ISMS
The periodic internal audit is a must for monitoring and review. Internal audit review consists of testing of controls and identifying corrective/preventive actions. To complete the PDCA cycle, the gaps identified in the internal audit must be addressed by identifying the corrective and preventive controls needed and the company's compliance based on a gap analysis.

To be effective, the ISMS needs to be reviewed by management at periodic, planned intervals. The review follows changes/improvements to policies, procedures, controls and staffing decisions. This important step in the process is project management review. The results of audits and periodic reviews are documented and maintained.

Phase 10—Prepare for the Certification Audit
In order for the organization to be certified, it is essential that it conduct a full cycle of internal audits, management reviews and activities in the PDCA process, and that it retains evidence of the responses taken as a result of those reviews and audits. ISMS management should review risk assessments, the RTP, the SOA, and policies and procedures at least annually.

An external auditor will first examine the ISMS documents to determine the scope and content of the ISMS. The objective of the review and audit is to have sufficient evidence and review/audit documents sent to an auditor for review. The evidence and documents will demonstrate the efficiency and effectiveness of the implemented ISMS in the organization and its business units.

Phase 11—Conduct Periodic Reassessment Audits
Follow-up reviews or periodic audits confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic reassessment audits to confirm that the ISMS continues to operate as specified and intended. As with any other ISO standard, ISO 27001 follows the PDCA cycle and assists ISMS management in knowing how far and how well the enterprise has progressed along this cycle. This directly influences the time and cost estimates related to achieving compliance.

CONCLUSION

The true success of ISO 27001 is its alignment with the business objectives and effectiveness in realizing those objectives. IT and other departments play an important role in implementing ISO 27001. Implementing ISO 27001 is an exercise toward better understanding an existing inventory of IT initiatives, information availability and ISMS implementation phases. An organization also needs to have the detailed understanding of PDCA implementation phases.

Without a well-defined and well-developed ISO 27001 project plan, implementing ISO 27001 would be a time- and cost-consuming exercise. To achieve the planned return on investment (ROI), the implementation plan has to be developed with an end goal in mind. Training and internal audit are major parts of ISO 27001 implementation.

ISO 27001 certification should help assure most business partners of an organization's status with respect to information security without the necessity of conducting their own security reviews. An organization would choose to be certified against the ISO 27001 standard to provide confidence to their customer base and partners.

AUTHOR'S NOTE

This article contains general information only, and Professional Consultant and the author are not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. Before making any decision or taking any action that may affect the business, consult a qualified professional advisor. Professional Consultant, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this article.

The author would like to thank Mary Holloway for her assistance.

ENDNOTES

[1] The ISO 27000 Directory, "The ISO 27001 Certification Process," *www.27000.org/ismsprocess.htm*

[2] The ISO 27000 Directory, "Introduction to ISO 27002," *www.27000.org/iso-27002.htm*

[3] ISO 27001 Security, "ISO/IEC 27001," *www.iso27001security.com/html/27001.html*

[4] Perera, Daminda, "ISO/IEC 27001 Information Security Management System," 26 July 2008, *www.daminda.com/downloads/ISO27001.pdf*

[5] Activa Consulting, "ISO 27001—Likely Costs," *www.iso-27001.co.uk/iso_27001_project_costs.htm*

[6] Schwartz, Mark S.; Thomas W. Dunfee; Michael J. Kline; "Tone at the Top: An Ethics Code for Directors?," *Journal of Business Ethics*, vol. 58, 2005, *http://lgst.wharton.upenn.edu/dunfeet/Documents/Articles/Tone%20At%20the%20TopJBE.pdf*

Rethinking Physical Security in the Information Age

Peter English, CISM, is corporate risk advisor for a local government in Scotland.

Two hundred and fifty years since the forces set in motion by the Industrial Age were unleashed, some of the effects, such as global warming, are only now beginning to be understood. After only 30 years, the Information Age is already profoundly changing all aspects of life and will continue to do so. Advanced electronic equipment and fast, cheap communications mean that many previously static aspects of daily life, including physical security, are lagging behind the new reality that has been created.

In the days before the Internet created a global information-sharing network, 'security through obscurity' was a more viable strategy. Now, those with criminal intent can go from zero to dangerous in 60 minutes by searching the Internet for a tutorial. The threat is not just from malware or hackers; physical security mechanisms are also at risk. From videos of how to open cars with a tennis ball to sites dedicated to opening so-called 'high-security' locks in seconds, key areas of the physical security environment may not be as secure as one would think.

Inscribed on the Temple of Apollo at Delphi (Greece) was the imperative to 'know thyself'. Organisations wishing to tackle the challenges of the future would do well to start from a position of self-awareness. One of the causes of the 'credit crunch' was that banks and regulators did not really understand the level of risk that they faced. Likewise, security officers need to understand the vulnerabilities, limitations and dependencies of information systems in order to successfully mitigate risks. While many organisations are getting better at identifying and understanding digital weaknesses, the inherent weaknesses of physical devices are not as well recognised. Certainly, uncontrolled physical access to computers can be devastating—a so-called 'evil maid' attack can cause the compromise of sensitive information.

In 2007, the German magazine *Der Spiegel* reported that Mossad agents broke into the London hotel room of a visiting Syrian official and planted malware on his laptop.[1] According to the magazine, information gleaned by the malware was used to degrade Syrian air defences in a bombing raid on an alleged nuclear facility. Even if an enterprise does not have a national air defence system to protect, it is worth understanding the limitations of its physical security devices because if the enterprise does not, its attackers more than likely will.

In February 2011, UK customers of Vodafone (a mobile telephone company) experienced problems accessing voice, text and mobile Internet services because of the theft of network equipment and IT hardware from a data centre that was broken into in the middle of the night.[2]

Just as computer hackers try to make systems perform in ways in which they are not supposed to, lock pickers try to do the same to a lock, i.e., by making it allow access to someone who does not have the correct key. For too long, lock-and-key security has been based on 'security through obscurity', with knowledge and tools carefully protected by locksmiths. However, the Internet has burst the obscurity bubble as thousands of people share information about weaknesses and bypasses for particular locks. Specialist tools are now available at high street prices and can be possessed in most countries without legal sanction. Why risk noisily jimmying a lock now that there are scores of web sites and videos dedicated to lock picking and lock 'bumping', which can help a person silently open a door in seconds? (Typing the name of a specific door lock and the 'bump key' [available for around US $10 plus shipping and handling] into a search engine is not for the faint-hearted.)

Researchers at the University of California, San Diego, USA, using off-the-shelf equipment and software, recently photographed a key from 200 feet above and successfully made a copy of it.[3] By proving that keys can be photographed from a distance and accurately copied, the researchers have undermined old assumptions about physical keys being 'secret'.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

It is, however, important not to focus too much on locks and doors because criminals are well practised at defying threat models. In response to car immobilizers, thieves started breaking into houses to steal the keys; a prolific burglar who was recently jailed in the UK defeated home security measures by removing tiles and then cutting his way in through roofs.[4] The less-imaginative crook could always use the tried-and-tested technique of smashing a hole in the drywall or a window.

Many security officers will be aware of certifications such as the Common Criteria and accompanying Evaluation Assurance Levels and will choose their equipment accordingly,[5] but, often, physical security items are purchased by another department without information security being considered. Physical security standards also exist. For example, in the UK, the Loss Prevention Certification Board (a collaboration amongst government, manufacturers and the insurance industry) tests the security claims of products to destruction according to Loss Prevention Standard 1175.[6] The standard's security levels range from 1 to 8—with a product security rated as 1 resisting entry for one minute to opportunistic attacks using limited tools up to a product security rated as 8, which is certified to resist entry for 20 minutes from professional attackers using extreme means with a wide range of tools (including electrically powered tools such as saws and drills).

Just as security officers would want to know exactly what a vendor means when it reports that a product is 'secure', so should physical security claims be queried and tested. Penetration testing physical security by seeing how much effort it requires to defeat a door or window is unlikely to be popular at any business, so using products based on the correct certification standards for one's country is important. A physical security asset that is certified to withstand, for example, 10 minutes of attack allows more accurate incident-response plans to be developed, such as reducing the gap between a break-in being detected and the time it takes for key holders or law enforcement to travel to the scene. Furthermore, certification standards help provide reasonable assurance to the organisation that its information assets are properly protected and allow some quantification of the organisation's ability to withstand an attack.

Depending on the severity of the threat environment faced, the UK government's information risk assessment guidance (Information Assurance Standard 1) refers to three levels of preparedness for computer systems: aware, detect and resist, and defend.[7] This categorisation could equally apply to physical security. At a minimum, security officers should be *aware* of the limitations of physical security (i.e., as the ancient Greeks advised, they should 'know themselves') and perhaps move sensitive assets to a different location or put in place compensating controls. Where sensitive assets are at risk, measures that will *detect* and *resist* attacks, i.e., those that are tamper-evident or alarmed, should be deployed. Finally, where assets are mission-critical, physical security measures that will *defend* those assets from unauthorised access for a certified level of time should be put in place.

Security officers are perpetually in a race with well-motivated threat actors, which is why layered security controls are important, but the profession tends to focus on the technical challenges to the detriment of the physical and, hence, overall security levels. No security officers worth their salaries would say 'the enterprise is fine because it has a firewall', and no security officers should be satisfied with the words 'that building is secure because it is kept locked'.

ENDNOTES

[1] Schneier, Bruce; 'Mossad Hacked Syrian Official's Computer', *Schneier on Security*, 5 November 2009, *www.schneier.com/blog/archives/2009/11/mossad_hacked_s.html*

[2] BBC News, 'Thousands Lose Vodafone Service', 28 February 2011, *www.bbc.co.uk/news/technology-12595681*

[3] Laxton, Benjamin; Kai Wang; Stefan Savage; 'Reconsidering Physical Key Secrecy: Teleduplication Via Optical Decoding', Association for Computer Machinery (ACM) Computer and Communications Security (CCS) conference, USA, October 2008, *http://vision.ucsd.edu/~blaxton/sneakey.html*

[4] BBC News, 'Prison for "Crime Show" Burglar', 26 September 2008, *http://news.bbc.co.uk/1/hi/england/nottinghamshire/7638909.stm*

[5] Common Criteria, *www.commoncriteriaportal.org*

[6] Red Book Live, 'Physical Security of Buildings', *www.redbooklive.com/page.jsp?id=306*

[7] National Technical Authority for Information Assurance, Her Majesty's Government Information Assurance (HMG IA) Standard No. 1, *Technical Risk Assessment*, issue 3.51, October 2009, UK, *www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf*

Measure and Monitor Application Security

Sivarama Subramanian, CISM, is senior architect of technology at Cognizant Technology Solutions, where he is currently overseeing the security initiatives for retail and retail e-commerce engagements. Subramanian is a member of the ISACA Chennai, India, Chapter and can be reached at *sivaramasubramanian.kailasam@cognizant.com.*

In the increasingly digitally connected world, information is the most valuable asset. Web applications are the gateway to access information, and they are no longer confined to a simple browser interface invoked from a laptop or desktop. With smartphones and smart TVs (televisions with a Wi-Fi or network connections) and appliances, applications are available everywhere.

This thrusts a lot of responsibilities on the security community to safeguard the interests of stakeholders and the information that is exchanged via web applications. The security community[1] has published best practices, guidelines and checklists to embed security into web applications. For example, one of the best practices is to call out specifically how to handle the SQL injection or to handle the cross-site scripting in the design document itself so that when the developers implement the design, the security is inherent in the code. Securing the system development life cycle (SDLC) is no longer a separate activity.

How does one ensure the effectiveness of application security? How are the security initiatives that minimize the risks and threats from hackers measured? This article attempts to define metrics that measure the effectiveness of application security in an organization.

DEFINE THE METRICS

Metrics are the prime indicators of management initiatives in any organization. Organizations witness a slow, but steady, increase in need for information security within. In many organizations, information security has attained a fairly considerable level of maturity. Web application security, as a part of the overall information security program, plays a major role in protecting valuable information. Therefore, the best time to define a metric is at the start of the application security program. The best possible approach is to:

- Identify the metrics.
- Identify the data-collection techniques.
- Obtain agreement from key stakeholders.
- Report the metrics to key stakeholders at the agreed-upon time interval.

The identified metrics should be useful to measure the effectiveness of the security program as well as to identify the gaps for future improvement.

There are two broad categories of metrics that can be captured for application security. The first set of metrics is for incidents and vulnerabilities (**figure 1**), and the second set is for the application security program itself (**figure 2**).

Figure 1—Metrics for Incidents and Vulnerabilities

Metric	Purpose
Number of incidents reported	Represents the number of incidents reported or discovered in the measurement window and helps identify the up/down trend of incidents
Number of incidents resolved	Helps identify the up/down trend of resolutions. Downtrend can be investigated, and timely corrective action can be taken.
Number of vulnerabilities reported	Represents the number of vulnerabilities reported or discovered in the measurement window and helps identify the up/down trend of vulnerabilities
Number of vulnerabilities resolved	Helps identify the up/down trend of resolutions. Downtrend can be investigated, and timely corrective actions, such as awareness training or focused reviews, can be taken.
Total security effort	Helps identify the effort spent on all the security activities. The idea is to reduce the effort by following a secure SDLC program.
Average effort—vulnerability assessment	Helps identify where the effort is being spent for resolving the incidents and vulnerabilities. The idea is to reduce the effort by following a secure SDLC program.
Effective ratio (number of reported vulnerabilities/number of found vulnerabilities)	Measures the defect leakage of the security program. If the value of the ratio is more than one, the program is not effective.

Figure 2—Metrics for the Application Security Program

Metric	Purpose
Number of proactive scans	Indicates how many automated scans are done for the web applications in the measurement window
Number of security awareness sessions	Indicates how many training sessions are conducted to impart the current trend of security risks and also the security awareness for new employees
Design review ratio (number of design reviews/total number of designs delivered)	Indicates whether all design documents have been reviewed. For example, if there are four design documents and only three reviews held, it means that the metric value is 0.75, or 75 percent. The metric value should be 1, or 100 percent to indicate that all the designs are reviewed.
Code review ratio (number of code reviews/total number of modules)	Indicates whether all source code has been reviewed. For example, if there are four modules and only three reviews held, it means that the metric value is 0.75, or 75 percent. The metric value should be 1, or 100 percent, to indicate that all the modules are reviewed.
Number of vulnerabilities prevented from proactive activities	Quantifies the effectiveness of the security reviews
Number of articles added to the knowledge base	Helps track updates to the knowledge base

COLLECT THE DATA

The data for the metrics should be collected on an ongoing basis (e.g., weekly, per event). The data collection template needs to be defined and kept in a centralized repository. As soon as the reviews are done, the review metrics can be updated in the data-collection template.

The incident's data can be collected from the incident database. The vulnerabilities and effort can be collected from the project team. The reviews and comments should be updated in a shared repository, and data are to be reported from the repository.

REPORT THE METRICS

At the end of the month, or as per the agreed-upon cutoff date with the project team, the data can be collated and presented. A few presentation examples are illustrated in **figures 3** and **4**.

Figure 3—Total Security Effort

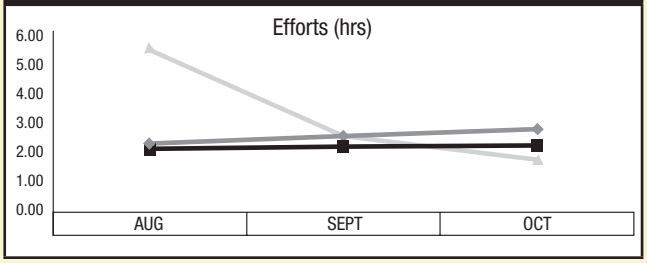
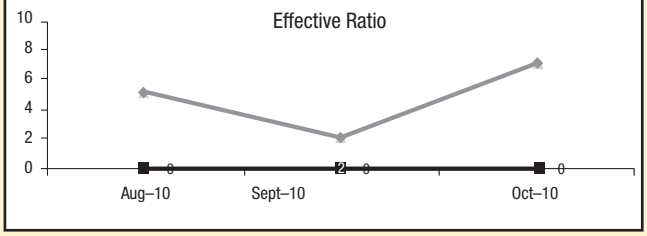


Figure 4—Effective Ratio



CASE STUDY

The following section offers a brief case study related to application security.

Problem Statement

The problem statement for the case example is: Manage the application security for the e-commerce applications of a pharmaceutical company by measuring the key metrics associated with application security.

The key metrics agreed upon for the measurement include:

- The number of vulnerabilities reported
- The number of vulnerabilities resolved
- Total security effort
- The number of security awareness sessions
- The design review ratio (number of design reviews/total number of designs delivered)

• The code review ratio (number of code reviews/total number of modules)

Implementation

After the key metrics were agreed upon by the senior management team, the kickoff meeting was scheduled with the project leadership team. The metrics were explained to the team, and a monthly measurement window was chosen. The data collection techniques were explained, and the schedule was given to the project leads.

At the end of the first measurement cycle, the data were collected and collated as shown in **figure 5**.

Figure 5—Data Collection and Collation

Metric	Units	December 2010
Number of vulnerabilities reported	Count	18
Number of vulnerabilities resolved	Count	15
Total security effort	Hours	80
Number of security awareness sessions	Count	1
Design review ratio (number of design reviews/total number of designs delivered)	Percentage	75
Code review ratio (number of code reviews/total number of modules)	Percentage	50

Business Benefit

The metrics were presented in the project-review meeting, and the project manager approved the data. **Figure 5** indicates that the secure code review process needs to be institutionalized; this would enable the project team to take corrective action and reduce further vulnerabilities. However, metrics should be collected for subsequent months to understand long-term trends.

CONCLUSION

With more stringent security controls in place for the infrastructure and networks of organizations, hackers are turning their attention to web applications. Through the vulnerabilities of web applications, the network and infrastructure can be compromised. Along with the increased adoption of cloud computing, there is more attention given to application security. The metrics discussed in this article should help organizations measure their application security postures. In this age of information, an organization needs to safeguard its information to have a competitive edge and to win the trust of key stakeholders.

ENDNOTES

[1] By "security community," the author is referring to groups such as the Open Web Application Security Project (OWASP), the Cloud Security Alliance and social media outlets.

The Assimilation of Marketing's Service Quality Principles and the IT Auditing Process

A Move Toward Quantifiable SAS 70 Auditing Service Quality, Part 2

Thomas J. Bell III, Ph.D., CISA, PMP, is a professor of business administration in the School of Business at Texas Wesleyan University in Fort Worth, Texas, USA, and an IT security auditor for *ComputerMinds.com* in Euless, Texas, USA. His IT auditing specialty is IT audits for small community banks (IT security audits and external penetration testing) and SAS 70 Type I and II audits.

Thomas Smith, Ph.D., is a professor of marketing and mass communication in the School of Business at Texas Wesleyan University in Fort Worth, Texas, USA. His publications include articles about advertising theories and practices in addition to creative marketing. He also has decades of service marketing experience.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

This article is the continuation of "The Assimilation of Marketing's Service Quality Principles and the IT Auditing Process: A Move Toward Quantifiable SAS 70 Auditing Service Quality, Part 1" (published in vol. 3, 2011), which suggests that broad quality auditing principles for organizations are realized through controlled processes and procedures. Increasingly, service businesses are finding that sustained profitability is related to delivering service quality. Delivering service quality seems to be a prerequisite for business success, or, at a minimum, a prerequisite for a business to stay afloat in an increasingly competitive market. Auditing procedures should deliver quality via processes that are defined, controlled, communicated and executed. Such processes contribute to the concept of continuous improvement.

However, to close the continuous improvement loop, W. Edwards Deming's plan-do-check-act (PDCA) model suggests that all processes must be measured iteratively, and SERVQUAL has proved to be an accepted instrument for measuring service quality across several service industries. SERVQUAL is an objective instrument for measuring service quality from the customer judgment vantage point.

The purpose of this article is twofold: to describe the development of a multiple-item scale for measuring service quality and to discuss SERVQUAL properties and assimilation with Statement on Auditing Standards (SAS) No. 70 auditing services. This topic is of importance because of the distinct challenges associated with measuring service quality attributes, which are unlike physical products with tangible characteristics that lend themselves to some form of measurement such as dimensions, appearance, texture, packaging and color. Understanding and measuring services can be significantly more difficult than understanding and measuring tangible products. Services have no physical attributes to measure; thus, the essential nature of the service should be considered from the customer's perspective.

SERVQUAL ASSIMILATION INTO SAS 70 AUDITING

Because of the elusive and abstract nature of quality and services, there is no objective measure to assess service quality. In the absence of an objective measure, the customers' perception of quality has been used as a measure to assess service quality.[1] An obvious way of obtaining a better understanding of customers' perceptions, needs and expectations is to ask them. However, prior to asking, it is useful to put some research into obtaining a view of an enterprise's services from its customers' perspective.

A. Parasuraman, Valarie A. Zeithaml and Leonard L. Berry defined service quality as a customer's judgment regarding the firm's excellence or superiority with emphasis on perceived quality as a defining factor of service quality.[2] According to Sylvie Llosa, Jean-Louis Chandon and Chiara Orsingher, service quality is an attitude or belief that is the result of expectations and perceived performance.[3] Customer assessment of service quality is often achieved by comparing the service that is actually experienced with the customer's expectations.[4] Alternatively stated, customers rate the quality of services by the gap between perceived and expected service.

The Reliability, Assurance, Tangible, Empathy and Responsiveness (RATER) multidimensional model[5] (**figure 1**) forms a structure of service quality sufficient for measuring SAS 70 service quality by using a performance and expectations

gap with the SERVQUAL (22 items) scale. This model can be used to identify and assess customer expectations, to plan and improve services and to measure customer satisfaction.

Figure 1—SERVQUAL RATER Model

Dimension	Description
Reliability	Ability to perform service dependably and accurately
Assurance	Ability of staff to inspire confidence and trust
Tangible	Physical facilities, equipment, staff appearance, etc.
Empathy	Extent to which caring, individualized service is given
Responsiveness	Willingness to help and respond to customer need

SERVQUAL: Reliability Dimension

Many businesses unwittingly use the terms "SAS 70 certified" or "SAS 70 compliant"; both terms are misnomers that, arguably, imply guarantees or the meeting of statutory or regulatory requirements. Specifically addressing this misnomer is central to the reliability dimension (service dependability and accuracy) of SERVQUAL. This begins with an understanding that a SAS 70 audit is only a guarantee that a third-party independent auditor was used to examine a company's IT security controls and related processes with documented findings in a SAS 70 report. The SAS 70 audit report includes the auditor's opinion or attestation statement issued to the service organization at the conclusion of a SAS 70 audit. This report is effectively an auditor-to-auditor communiqué between the service and user organization (the entity that has engaged a service organization—particularly if its financial statements are impacted by the services of the service organization).

The reliability of the SAS 70 report may lie in its not being complicit in the misuse of the report by some vendors using the report to support exaggerated marketing claims. Requests from service vendors to prepare SAS 70 reports for purposes that are outside the intended scope of the reports should be refused or avoided. SAS 70 reports were not intended to supplant good old-fashioned IT security due diligence on the part of service vendors, nor should it; only present-day observations are noted without indicating any forward-looking representations.

SERVQUAL: Assurance Dimension

An old adage holds that people are judged by the company they keep. If one subscribes to this truism, audit firms are well served to surround themselves with people who share their ideals and values. Inspiring confidence and trust as it relates to the assurance dimension is about creating an organization of character that delivers on its commitments—an organization that is attuned to answering the needs of others and that is willing to go the extra mile to support its customers. Another way to engender confidence and trust is to utilize an organization that is known for exceptional products and services and that is respected or admired in the marketplace.

Beyond platitudes (i.e., "customers come first") of the normal business rhetoric, earning trust is a journey achieved over time; customer trust is the most direct route to long-term success, as demonstrated time and time again by successful businesses. Inspiring trust is accomplished in small increments one customer at a time, improving a single process as needed. Bill Price and David Jaffe suggest checklists of things to do and not do when operating an interaction center and provide the right choices for customers at every point in the service process:[6]

- On the web site, phone numbers should appear on every page. "Talk to someone" or "chat" buttons should be utilized, and a "contact us" button should be available to make it easy to send e-mails and should state how quickly customers should expect a response.
- For interactive voice response phone menus or trees, web site alternatives should be clearly mentioned; the option to leave a callback number should be provided; and at any point, the caller should be able to hit 0 to reach an operator.
- E-mails to customers should always provide an accompanying phone number, along with links to pages on the web site that can actually help explain the issue(s).
- There should be branch operations that have phones for calling the contact center directly, self-service desks for information, and web-enabled personal computers (PCs) for direct self-service online. Make it easy to contact the enterprise, not difficult.

- Eliminate "dumb" contacts and unnecessary repeated contacts through better processes and information.
- Create engaging self-service so that customers can help themselves when possible.
- Be proactive; do not wait for trouble.
- Address and fix ownership of problems; do not assign blame to someone else.
- Listen to the customers, and learn from their feedback and comments.
- Assist customers when they need help.

According to Price and Jaffe, in general, people will not pay for services or purchase products if they do not trust the company or have confidence in its service.[7] Customers will develop trust only if they judge that their interactions with a company are efficient and customer-oriented. Customer interaction is a dominant form of service offered by service companies, yet it is still a nascent discipline for most business people—with lots of unknown complications and unappreciated benefits.

SERVQUAL: Tangible Dimension

For auditors, the tangible dimension is based largely on facility and staff appearance. Looking professional is essential to being respected and successful in business environments. Understanding what one's attire is communicating and how best to represent oneself and one's company during an audit engagement can influence customer perception.

A polished personal image is as important as an *organization's* polished image. Proper business attire should be followed irrespective of age, gender or client. Queen Elizabeth II of England is reported to have said, "Dress gives one the outward sign from which people can judge the inward state of mind. One they can see, the other they cannot." Expectations in dress may vary, but when in doubt, it is always best to dress slightly more formally than may be necessary. Overdressing may make a positive impression on your peers or superiors; underdressing may be perceived as lacking professionalism, savvy or competence.

SERVQUAL: Empathy Dimension

Extending caring, individualized service is a critical element for success, as it is all about retention—keeping customers inside the loyalty loop as long as possible. Research indicates that improving retention rates can increase profitability.[8]

A SAS 70 audit should be a security awareness process that engages and educates the customer in ways to better secure the organization's IT resources. A broad base of informed workers is a cost-effective way to mitigate security risks and better assist auditors. To bring about security awareness, auditors must be willing to relinquish a measure of control as they learn to facilitate risk reduction through effective communication. Once customers are empowered to realize that they have the resources and authority to better safeguard the organization's information assets, their actions could respond accordingly. An essential part of developing security awareness is to engage the auditee and allow the auditor to experience a paradigm shift—in which auditors begin to comprehend the problems they unintentionally create by their mere presence. Such actions epitomize empathy while individualizing services to the customer's vantage point.

SERVQUAL: Responsiveness Dimension

The responsiveness dimension examines an auditor's willingness to help and respond to customer needs. Responsiveness encompasses an auditor's objectivity; soft skills; and some general understanding of the social psychology of conducting a security audit and the need to understand the customer's thoughts, feelings, behaviors and influences.

The human psychology of the audit client or customer (when collecting and evaluating evidence of an organization's information systems, practices and operations) is often overlooked, with emphasis usually placed on the process and not the customer. Arguably, auditing is a human relationship business. As such, auditors should understand the social psychology or the people-side of auditing, beyond the standards, procedures and best practices. Clearly, it is important to understand the process of obtaining and evaluating evidence to determine whether an information system adequately safeguards assets and maintains data integrity while operating effectively and efficiently to achieve the organization's goals and objectives.

However, understanding the social psychology of IT security auditing is as important as the auditing processes and procedures. Persuading audit clients to become more security-conscious may involve finding ways to overcome auditing anxiety by effectively communicating with customers and letting them know what they are expected to do and what the auditor is willfully doing to support their efforts to reasonably safeguard the organization's information assets.[9]

SERVQUAL, A METHODOLOGY FOR MEASURING SERVICE QUALITY

As a way of trying to measure service quality, researchers developed SERVQUAL, a perceived service quality questionnaire survey methodology. SERVQUAL examines five dimensions of service quality:

1. Reliability
2. Assurance
3. Tangible
4. Empathy
5. Responsiveness

For each dimension of service quality, SERVQUAL measures both the expectation and perception of the service on a scale of 1 to 7, with 22 questions in total. Each of the five dimensions is then weighted according to customer importance, and the score for each dimension is multiplied by the appropriate weighting.

Following this, the gap score for each dimension is calculated by subtracting the expectation score from the perception score. A negative gap score indicates that the actual service (the perceived score) was less than what was expected (the expectation score).

The gap score is a reliable indication of each of the five dimensions of service quality. Using SERVQUAL, service providers can obtain an indication of the level of quality of their service provision and highlight areas requiring improvement.

The Methodology

In this sample SERVQUAL survey, a SAS 70 audit firm is surveyed; however, any service organization can be surveyed using the provided template. All that needs to be done is to substitute the phrase "SAS 70 audit firm" with the particular organization or industry being surveyed. The steps for carrying out a SERVQUAL survey are:

1. Select the SAS 70 audit firm whose service quality is to be assessed. Using the questionnaire (**figures 2** and **3**), obtain the score for each of the 22 expectation statements and then the score for each of the 22 perception statements.

Figure 2—Customer Expectations (SERVQUAL Survey)

This section of the survey deals with your opinions of SAS 70 audit firms. Please show the extent to which you think SAS 70 audit firms should possess the following features. Provide a number between 1 and 7 that best shows your expectations about institutions offering SAS 70 auditing services. Rank each statement as follows.

Strongly Disagree						Strongly Agree	
1	2	3	4	5	6	7	
Statement							**Score**
1.	Excellent SAS 70 audit firms will have modern-looking equipment.						
2.	The physical facilities at excellent SAS 70 audit firms are visually appealing.						
3.	Employees at excellent SAS 70 audit firms are neat in their appearance.						
4.	Materials associated with the service (pamphlets or statements) will be visually appealing at an excellent SAS 70 audit firm.						
5.	When excellent SAS 70 audit firms promise to do something by a certain time, they do.						
6.	When a customer has a problem, excellent SAS 70 audit firms will show a sincere interest in solving it.						
7.	Excellent SAS 70 audit firms will perform the service right the first time.						
8.	Excellent SAS 70 audit firms will provide the service at the time they promise to do so.						
9.	Excellent SAS 70 audit firms will insist on error-free records.						
10.	Employees of excellent SAS 70 audit firms will tell customers exactly when services will be performed.						
11.	Employees of excellent SAS 70 audit firms will give prompt service to customers.						
12.	Employees of excellent SAS 70 audit firms are always willing to help customers.						
13.	Employees of excellent SAS 70 audit firms will never be too busy to respond to customer requests.						
14.	The behavior of employees in excellent SAS 70 audit firms will instill confidence in customers.						
15.	Customers of excellent SAS 70 audit firms will feel safe in transactions.						
16.	Employees of excellent SAS 70 audit firms are consistently courteous with customers.						
17.	Employees of excellent SAS 70 audit firms will have the knowledge to answer customer questions.						
18.	Excellent SAS 70 audit firms will give customers individual attention.						
19.	Excellent SAS 70 audit firms will have operating hours convenient to all their customers.						
20.	Excellent SAS 70 audit firms will have employees who give customers personal service.						
21.	Excellent SAS 70 audit firms will have their customers' best interests at heart.						
22.	The employees of excellent SAS 70 audit firms will understand the specific needs of their customers.						

Figure 3—Customer Perceptions (SERVQUAL Survey)

The following statements relate to your feelings about the particular SAS 70 audit firm chosen. Please show the extent to which you believe this SAS 70 audit firm has the feature described in each statement. Provide a number between 1 and 7 that best shows your perceptions about the specific SAS 70 audit firm. Rank each statement as follows.

Strongly Disagree						Strongly Agree	
1	2	3	4	5	6	7	
Statement							**Score**
1.	The SAS 70 audit firm has modern-looking equipment.						
2.	The SAS 70 audit firm's physical features are visually appealing.						
3.	The SAS 70 audit firm's employees are neat in appearance.						
4.	Materials associated with the service (such as pamphlets or statements) are visually appealing at the SAS 70 audit firm.						
5.	When the SAS 70 audit firm promises to do something by a certain time, it does so.						
6.	When you have a problem, the SAS 70 audit firm shows a sincere interest in solving it.						
7.	The SAS 70 audit firm performs the service right the first time.						
8.	The SAS 70 audit firm provides its service at the time it promises to do so.						
9.	The SAS 70 audit firm insists on error-free records.						
10.	Employees at the SAS 70 audit firm tell you exactly when the services will be performed.						
11.	Employees at the SAS 70 audit firm give you prompt service.						
12.	Employees at the SAS 70 audit firm are always willing to help you.						
13.	Employees at the SAS 70 audit firm are never too busy to respond to your request.						
14.	The behavior of employees at the SAS 70 audit firm instills confidence in you.						
15.	You feel safe in your transactions with the SAS 70 audit firm.						
16.	Employees at the SAS 70 audit firm are consistently courteous to you.						
17.	Employees at the SAS 70 audit firm have the knowledge to answer your questions.						
18.	The SAS 70 audit firm gives you individual attention.						
19.	The SAS 70 audit firm has operating hours convenient to all its customers.						
20.	The SAS 70 audit firm has employees who give you personal service.						
21.	The SAS 70 audit firm has your best interests at heart.						
22.	The employees of the SAS 70 audit firm understand your specific needs.						

Calculate the gap score (perception minus expectation) for each of the statements (**figure 4**).

2. Obtain an average gap score for each dimension of service quality by assessing the gap score for each of the statements that constitute the dimension and dividing the sum by the number of statements making up the dimension (**figure 4**).
3. Sum the averages calculated in step 2, and divide by five to obtain an average SERVQUAL score. This score is the unweighted measure of service quality for the area being measured.
4. For a weighted score, calculate the importance weight for each of the five dimensions of service quality constituting the SERVQUAL scale. The sum of the weights should add up to 100 (**figure 5**).
5. Calculate the weighted average SERVQUAL score for each of the five dimensions of service quality by multiplying the averages calculated in step 2 by the weighted scores calculated in step 4 (**figure 6**).
6. Sum the scores calculated in step 5 to obtain the weighted SERVQUAL score of service quality for the area being measured.

SERVQUAL Survey

The survey is broken into two sections. In the first section (**figure 2**), respondents rank all SAS 70 audit firms according to the their expectations, i.e., what they expect all SAS 70 audit firms to provide. In the second section (**figure 3**), respondents rank the SAS 70 audit firm chosen for the survey according to their experiences and perceptions.

CONCLUSION

Since, unlike physical products, services are considered processes or performances with obscure or abstract characteristics, there is no objective measure to assess service quality.[10] In the absence of an objective measure, customers' perceptions of quality have been used as a measure to assess service quality across several industries including auditing.[11] The multidimensional structure of service quality is perhaps best measured by using performance and expectations gaps as measured by a SERVQUAL scale, which uses five dimensions across a 22-item survey instrument. SERVQUAL is increasingly being used for measuring service quality[12] because of its practical implication and its diagnostic

Figure 4—Calculation of SERVQUAL Scores					
Dimension	**Statement**	**Expectation Score**	**Perception Score**	**Gap Score**	**Average for Dimension**
Tangible	1				
	2				
	3				
	4				
Reliability	5				
	6				
	7				
	8				
	9				
Responsiveness	10				
	11				
	12				
	13				
Assurance	14				
	15				
	16				
	17				
Empathy	18				
	19				
	20				
	21				
	22				
Unweighted average SERVQUAL score:					

Figure 5—SERVQUAL Importance Weights	
Allocate 100 points among the five sets of features listed here according to how important the features are to you. Ensure that the points add up to 100.	
Features	**Points**
1. The appearance of the SAS 70 audit firm's physical facilities, equipment, personnel and communication materials	
2. The SAS 70 audit firm's ability to perform the promised service dependably and accurately	
3. The SAS 70 audit firm's willingness to help customers and provide prompt service	
4. The knowledge and courtesy of the SAS 70 audit firm's employees and their ability to convey trust and confidence	
5. The caring, individual attention the SAS 70 audit firm provides to its customers	
Total:	100

Figure 6—Calculation of Weighted SERVQUAL Scores			
SERVQUAL Dimension	**Score (from figure 2)**	**Weighting (from figure 3)**	**Weighted Score**
Tangibility			
Reliability			
Responsiveness			
Assurance			
Empathy			
Average weighted score:			

nature for improving service quality.[13] The SERVQUAL scale is a reliable and valid tool for measuring service quality of audit firms. Research findings indicate that the SERVQUAL scale consisting of five dimensions is reasonably satisfactory to measure perceived service quality of audit firms.

According to Z. Turk and Mutlu Yuksel Avcilar, assurance is the most important dimension of the service quality of audit firms, followed by reliability, responsiveness, empathy and tangibles.[14] These findings indicate that customers are more concerned with the assurance, reliability and responsiveness dimensions in assessing the service quality of audit firms.

One could surmise that audit firms seeking long-term sustainability should strategically focus on employees' knowledge, courtesy, ability to perform promised services dependably and accurately, and ability to help customers while providing services willfully in order to improve service quality.

ENDNOTES

[1] Bamert, Thomas; Hans Peter Wehrli; "Service Quality as an Important Dimension of Brand Equity in Swiss Services Industries," *Managing Service Quality*, vol. 15, issue 2, 2005

[2] Parasuraman, A.; V.A. Zeithaml; L.L. Berry; "SERVQUAL: A Multiple-item Scale for Measuring Consumer Perceptions of Service Quality," *Journal of Retailing*, vol. 64, issue 1, 1988

[3] Llosa, Sylvie; Jean-Louis Chandon; Chiara Orsingher; "An Empirical Study of SERVQUAL's Dimensionality," *The Service Industry Journal*, vol. 18, issue 2, 1998

[4] Donnelly, M.; M. Wisniewski; J.F. Dalrymple; A.C. Curry; "Measuring Service Quality in Local Government: The SERVQUAL Approach," *International Journal of Public Sector Management*, vol. 8, issue 7, 1995

[5] *Op cit*, Parasuraman, 1988

[6] Price, Bill; David Jaffe; *The Best Service Is No Service: How to Liberate Your Customers From Customer Service, Keep Them Happy and Control Costs*, USA, Jossey-Bass, 2008

[7] *Ibid.*

[8] Rust, Roland; Anthony Zahorik; "Customer Satisfaction, Customer Retention, and Market Share," *Journal of Retailing*, vol. 69, number 2, Summer 1993

[9] Bell, Thomas; "The Social Psychology of IT Security Auditing From the Auditee's Vantage Point: Avoiding Cognitive Dissonance," *ISACA Journal*, vol. 3, 2010

[10] Lovelock, C.H.; *Service Marketing, 2nd Edition*, Prentice Hall International, USA, 1991

[11] *Op cit*, Bamert, 2005

[12] Cui, Charles Chi; Barbara R. Lewis; Won Park; "Service Quality Measurement in the Banking Sector in South Korea," *International Journal of Bank Marketing*, vol. 21, issue 4, 2003

[13] Zhou, Lianxi; "A Dimension-specific Analysis of Performance-only Measurement of Service Quality and Satisfaction in China's Retail Banking," *Journal of Services Marketing*, vol. 18, issue 7, 2004

[14] Turk, Z.; Mutlu Yuksel Avcilar; "The Effects of Perceived Service Quality of Audit Firms on Satisfaction and Behavioural Intentions: A Research on the Istanbul Stock Exchange Listed Companies," *Research Journal of Business Management*, vol. 3, issue 1, 2009

Prepare for the **2011** CISM Exams

ORDER NOW—2011 CISM Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Security Manager® (CISM®) exam, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses.

www.isaca.org/cismreview

To order CISM review material for the December 2011 exam, visit the ISACA web site at *www.isaca.org/cismbooks* or see pages S1-S8 in this *Journal*.

CISM® Review Manual 2011—*ISACA*

Newly updated, the *CISM Review Manual 2011* is a comprehensive reference guide designed to assist individuals in preparing for the CISM exam and individuals who wish to understand the roles and responsibilities of an information security manager. The manual has been continually enhanced over the past six editions and is a current, comprehensive, peer-reviewed information security management global resource.

The 2011 edition assists helps candidates study and understand essential concepts in the following job practice areas:

- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

The *CISM Review Manual 2011* retains the easy-to-navigate format first introduced in 2010. Each of the book's five chapters has been divided into two sections for focused study. The first section contains the definitions and objectives for the five areas, with the corresponding tasks and knowledge statements that are tested on the exam.

Section one of each chapter is an overview that provides:

- Definitions for the five areas
- Objectives for each area
- Descriptions of the tasks
- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in section two for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section two of each chapter consists of reference material and content that support the knowledge statements. The material enhances CISM candidates' knowledge and/or understanding when preparing for the CISM certification exam. Also included are definitions of terms most commonly found on the exam.

This manual is effective as a stand-alone document for individual study and as a guide or reference for study groups and chapters conducting local review courses. It is also a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.

CM-11 English Edition **CM-11J** Japanese Edition **CM-11S** Spanish Edition

CISM® Review Questions, Answers & Explanations Manual 2011—*ISACA*

The *CISM Review Questions, Answers & Explanations Manual 2011* compiles 650 multiple-choice study questions that have previously appeared in the *CISM Review Questions, Answers & Explanations Manual 2009*, the *2009 Supplement* and the *2010 Supplement* into one effective resource. These questions are not actual exam items, but are intended to provide the CISM candidate with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISM Review Manual 2011.*

To help exam candidates maximize—and customize—their study efforts, questions are presented in the following two ways:

- Job practice area—Questions, answers and explanations are sorted by the current CISM job practice areas. This allows the CISM candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.
- Sample 200-question exam—200 of the 650 questions included in the manual are selected to represent a full-length CISM exam, with questions chosen in the same percentages as the current CISM job practice areas. Candidates are urged to use this sample test to simulate an actual exam, but also to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.

CQA-11 English Edition **CQA-11J** Japanese Edition **CQA-11S** Spanish Edition

CISM® Review Questions, Answers & Explanations Manual 2011 Supplements—*ISACA*

Newly created each year, the *CISM Review Questions, Answers & Explanations Manual 2011 Supplement* features 100 new sample questions, answers and explanations to help candidates effectively prepare for the 2011 CISM exam. These new questions are designed to be similar to actual exam items. The questions are intended to provide CISM candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISM exam. This publication is ideal to use with the *CISM Review Questions, Answers & Explanations Manual 2011*.

CQA-11ES English Edition **CQA-11JS** Japanese Edition **CQA-11SS** Spanish Edition

CISM® Practice Question Database v11—*ISACA*

The comprehensive CISM Practice Question Database v11 combines the *CISM Review Questions, Answers & Explanations Manual 2011* with the *CISM Review Questions, Answers & Explanations Manual 2011 Supplement* into a single 750-question study guide. Exam candidates can take sample exams with randomly selected questions and view the results by job practice, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CISM candidates to easily and quickly identify their strengths and weaknesses, and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions, giving candidates the ability to customize their study approach to fit their needs. The database software is available in CD-ROM format or as a download.

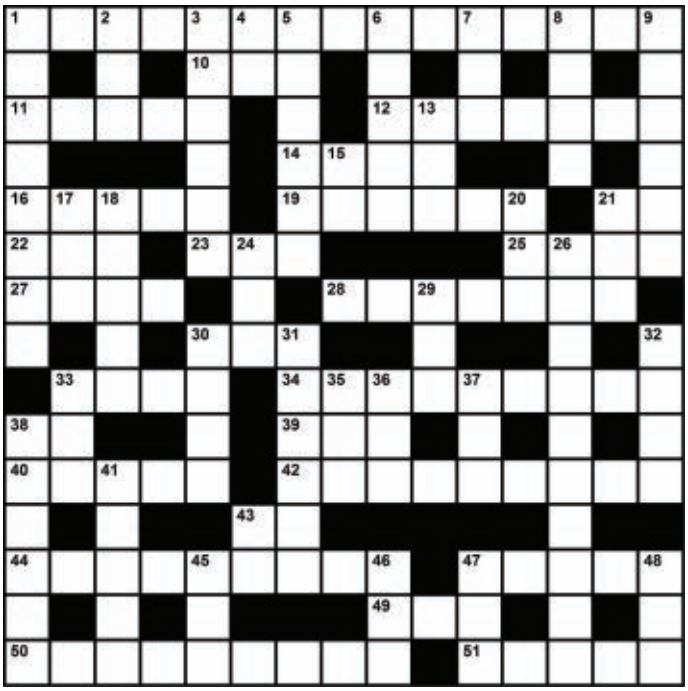
PLEASE NOTE the following system requirements:

- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP; Windows 7
- Microsoft .net Framework 3.5
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

MDB-11 English Edition—CD-ROM **MDB-11W** English Edition—Download

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS
1 One of the major concerns in disaster preparedness (2 words)
10 Interface abbr.
11 One of the members of ISACA's EU Regional Council who pioneered the creation of COBIT, ___ Dovran
12 LTO 5 technology aka
14 Increased
16 Relative magnitude
19 _____ crunch
21 ___ ratio
22 Identify
23 Expected
25 Back
27 First name of one of the founding pioneers of COBIT
28 Set straight
30 Set a goal
33 Reporting the right information at the right time to the right executives is one of its challenges (abbr.)
34 Intention to accomplish
38 Read only, abbr.
39 Life summary
40 Incident
42 One of the original information criteria of COBIT development
43 Safety testing and certification org., for short
44 Hackers, phishing and virus initiators, etc.
47 Big Four first name
49 Take a wrong turn
50 When it comes to risk management better than reactive
51 Part of SSL

DOWN
1 The D in DRP
2 Connection
3 Listed in order of importance
4 Old record
5 Penetrate security defenses, for example
6 Being worked with (2 words)
7 Germane
8 Set of concepts and practices for managing information technology services, development and operations, abbr.
9 Figure
13 Had an edge
15 Word of indecision
17 Hybrid, for one
18 Mentally quick and adaptable
20 The "___angulated Pendulum"
21 Wages
24 Prefix with lateral
26 Another of the original information criteria in COBIT development
29 Suggestion
30 Plugging away (2 words)
31 Control and use of these devices is one of AICPA's top 10 technology initiatives
32 Count on
33 US Homeland Security e-mail address ending
35 One of a series of ranges of values for a particular variable
36 Write down
37 Part of a machine
38 Overhaul
41 Amazon's cloud service (2 words)
43 Great Britain, abbr.
45 ____TE, Inter-American Committee Against Terrorism, abbr.
46 Watch
47 Emergency response level, abbr.
48 Prescription notation

(Answers on page 54)

HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Gan Subramaniam, CISA, CISM, CCNA, CCSA, CIA, CISSP, ISO 27001 LA, SSCP, is the global IT security lead for a management consulting, technology services and outsourcing company's global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big Four professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam's previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK; Thomas Cook (India); and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Q My employer recently bought one of our competitors, and integration between the two entities is occurring now. One of the key challenges is that the two entities use completely different and incompatible IT systems. Our audit team has been assigned the task of auditing the integration project and reporting to the leadership on the effectiveness of the approach used for integration. The business objective is to combine the positives from both systems into one. One of the major drivers behind the purchase was that the IT systems of the competitor were far superior to ours and were providing them an edge in terms of customer service delivery.

Can you help me with a quick checklist that I can use for my work?

A Whenever an acquisition happens, the target organisation feels vulnerable in terms of continued use of its systems and processes. There is a lot of cultural integration that needs to take place. Setting aside all those issues, let us try to develop a checklist that you may use to audit the IT systems integration project. As always, please note that this list is indicative only, and not exhaustive:

- An inventory of all the IT systems and applications should exist comprising all those used by both the entities. This inventory must include the complete details of the applications—platform, whether in-house developed/maintained or a third-party-supplied application, etc. It can be packaged software or customized packaged software. All such details must be gathered.
- An inventory of all the business processes in place must also exist.
- Various business processes have to be mapped with the different IT systems used.
- It should not be difficult to gather the inventory lists discussed in the previous bullets. If the entities have good business continuity plans in place, they will have the same automatically developed and used as part of business continuity management.
- When assessing the business processes at both entities, a decision has to be made about which of the processes will continue to be used. It may also be possible that the new merged entity may have a different set of processes developed to suit the new and changed environment. Once this decision is made, an inventory of the to-be-used processes—the previously used and to-be-developed—must be created.
- The newly developed process inventory must now be used to map the IT systems in use and bucket them into the following categories, making some key decisions on future systems use:
  - Systems that may be shelved
  - Systems that may continue to be used without any changes
  - Systems that may continue to be used with changes made to them
  - Systems that may be required to be developed new

Once this list is available, the rest of the work is relatively simple, though not easy. (Simple and easy may sound synonymous, but, in reality, they are not!) The next steps are:

- Given that systems and applications undergo continuous changes, a change freeze must be put in place immediately. A change freeze means that none of the systems and applications will undergo any changes in terms of either fault fixing or enhancements. Lack of a change freeze will lead to chaos.
- There should be a robust testing environment to support comprehensive testing on the various changes made to the different systems and applications.
- Change management processes, if any, ought to be audited in order to check their effectiveness. In particular, those relating to system go-live after the testing of various changes must be audited.
- It is essential to revisit the continuity plans or disaster recovery plans for the various IT systems used prior to the commencement of the integration work. Required improvements must

be made to the plans to make them complete, so that if any of the systems fail during the integration work, they can be recovered appropriately to ensure continuity of business operations.

- The major assumption here is that all the systems and applications are supported, managed and hosted in an in-house environment. This need not be the case on all occasions. Steps must be taken to assess the third-party vendor-operated environment, and, if necessary, the enterprise may choose to bring those systems in-house. Such transitions carry a different set of risks.
- Changes that ought to be made to facilitate integration alone must be made. Change freeze will ensure that no other changes are made.
- Integration of the IT systems should commence only after putting in place a conducive environment in terms of supporting processes and controls. Needless to say, appropriate programme management processes and controls aimed to ensure the proper execution and completion of various processes must be in place.
- Governance processes that monitor the integration work must be in place, and the progress must be measured using appropriate metrics. The stakeholders from both organisations—prior to the merger—must find a place in the governance structure.
- It is assumed that the IT organisation has done assessments on both environments with an aim to co-develop a new environment, fit for purpose in terms of the changed organisation.
- Continuous audit of the integration programme, until completion, is recommended. Then, a post-integration audit should take place, given the impact should the programme fail.

Q&A

Prepare for the **2011** CGEIT and CRISC Exams

ORDER NOW—2011 CGEIT and CRISC Review Materials for Exam Preparation and Professional Development

To pass the Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) exams, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses (*www.isaca.org/cgeitreview*).

CGEIT® Review Manual 2011
ISACA

The updated *CGEIT Review Manual 2011* is a detailed reference guide designed to help individuals prepare for the CGEIT exam and understand the roles of those who implement the governance of IT and have significant management, advisory or assurance responsibilities. The manual has been developed and reviewed by subject matter experts actively involved in the governance of IT worldwide.

The 2011 edition includes six chapters devoted to the domains within the scope of the CGEIT job practice:
- IT governance framework
- Strategic alignment
- Value delivery
- Risk management
- Resource management
- Performance measurement

Each chapter features task and knowledge statements with supporting explanations and exhibits detailing their interrelationships. Sample practice questions and explanations of answers assist candidates in effectively preparing for the 2011 CGEIT exam. Also included are definitions of terms typically found on the exam and references for further study.

The manual is an excellent resource for those seeking global guidance and a strong understanding of effective approaches to the governance of IT. It can be used for individual exam study or as a guide for group study. It also serves as a useful desk reference that can be added to the libraries of professionals involved in the governance of IT.

CGM-11 English Edition

CGEIT® Review Questions, Answers & Explanations Manual 2011
ISACA

CGEIT Review Questions, Answers & Explanations Manual 2011 is designed to provide CGEIT candidates with an understanding of the type and structure of questions and content that will appear on the CGEIT exam, the new *CGEIT® Review Questions, Answers & Explanations Manual 2011* consists of 50 multiple-choice study questions. To help candidates maximize study efforts, questions are sorted by domain, allowing CGEIT candidates to focus on particular topics, as well as scrambled as a sample 50-question exam, enabling candidates to effectively determine their strengths and weaknesses and allowing them to simulate an actual exam.

CGQ-11 English Edition

Candidate's Guide to the CGEIT ®Exam and Certification
ISACA

Candidate's Guide to the CGEIT Exam and Certification is supplied to individuals upon receipt of the CGEIT exam registration form and payment. This guide provides a detailed outline of the process and content areas covered on the examination, information on the exam's administration, and a sample copy of the answer sheet used for the exam.

CACG

Certified in the Governance of Enterprise IT® An ISACA® Certification

CRISC™ Review Manual 2011
ISACA

The new *CRISC™ Review Manual 2011* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The 2011 edition has been developed by global subject matter experts to assist candidates in understanding essential concepts of the CRISC job practice areas:
- Risk identification, assessment and evaluation
- Risk response
- Risk monitoring
- IS control design and implementation
- IS control monitoring and maintenance

The *CRISC Review Manual* features a unique learning format for focused study and is separated into two distinct parts.

Part I provides a thorough overview of the concepts related to the IT-related risk management process and the design, implementation, monitoring and maintenance of information systems (IS) controls. Each chapter contains the definitions and objectives for the five CRISC job practice domains, with the corresponding tasks performed by the risk management professional and the knowledge that is tested on the exam. Part I also includes sample practice questions, explanations of the answers and suggested resources for further study.

Part II describes, in detail, selected business and IT processes and how they relate to enterprise risk. For each of the selected processes it:
- Explains the process's importance to achieving business objectives
- Introduces related key concepts
- Provides real-life examples of common risks
- Lists selected key risk indicators
- Describes examples of common IS controls supporting the process
- Features the practitioner's perspective
- Offers suggested reading materials and references

This manual is an excellent stand-alone document for individual study and can be used as a guide or reference for study groups and chapters conducting local review courses.

CRR-11 English Edition

CRISC™ Review Questions, Answers & Explanations Manual 2011
ISACA

CRISC Review Questions, Answers & Explanations Manual 2011 is designed to provide CRISC candidates with an understanding of the type and structure of questions and content that will appear on the CRISC exam. The new *CRISC Review Questions, Answers & Explanations Manual 2011* consists of 100 multiple-choice study questions. To help candidates maximize study efforts, questions are sorted by domain, allowing CRISC candidates to focus on particular topics, as well as scrambled as a sample 100-question exam, enabling candidates to effectively determine their strengths and weaknesses and allowing them to simulate an actual exam.

CRQ-11 English Edition

Candidate's Guide to the CRISC™ Exam and Certification
ISACA

Candidate's Guide to the CRISC Exam and Certification is supplied to individuals upon receipt of the CRISC exam registration form and payment. This guide provides a detailed outline of the process and content areas covered on the examination, information on the exam's administration, and a sample copy of the answer sheet used for the exam.

CACR

Certified in Risk and Information Systems Control™ An ISACA® Certification

CPE Quiz

Prepared by Sally Chan,
CGEIT, ACIS, CMA

QUIZ #137

Based on Volume 2, 2011—Risk Management—What Is Your Capacity?

Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

ROSS ARTICLE

1. Return on security investment (ROSI) does not deal with the payback for individual outlays for equipment, software or services that safeguard information.
2. The value of an organization's intellectual property is tied to that of its information security. The techniques for assessing value of intellectual property include a cost approach and the aggregate expenditure to develop it.

SINGLETON ARTICLE

3. The American Institute of Certified Public Accountants (AICPA) states that audit services are reserved for financial audit, and thus, what the service auditor does is attest. Attest services are very definitive; management identifies specific procedures and the auditor then performs exactly those procedures.
4. A noteworthy difference between SAS 70 and SOC-1/SSAE 16 is the users of the report. SAS 70 was designed for multiple users and basically went into the public domain. SOC-1/SSAE 16 restricts use of the report to service/user managements and user auditors; that is, it cannot be used as a marketing tool to prospects.
5. The SOC-3 report is intended for use by stakeholders such as customers, regulators, business partners, suppliers and directors, whereas SOC-2 is for anyone interested.

JEGOUSSE ARTICLE

6. One of the proposed steps to identify the target application for further analysis is to schedule a workshop with representation from both the business and the controls assessment team and to start the workshop by restating the objective and describing the problem in terms of costs and compliance.
7. When contemplating the option of control reevaluation, whereby the application system controls are substituted to a strong manual control, the selling point is that, in instances such as weak IT controls with limited use of automated controls, it is often cheaper and more effective to implement key manual controls rather than rely on automation.

FISCHER ARTICLE

8. Approaches to IT risk scenarios—top down or bottom up—are not complementary. The approaches should be used sequentially.
9. The importance of risk factors lies in the influence they have on IT risk. They are heavy influencers of the frequency and impact of IT scenarios and should be taken into account during every risk analysis, when frequency and impact are assessed.
10. Scenarios expand one's thinking, uncover inevitable or near-inevitable futures, and protect against "groupthink." They help executives ask better questions and prepare for the unexpected.

PIRONTI ARTICLE

11. There are numerous methods and practices that can be used to evaluate the information security and risk management (ISRM) program and capabilities of an organization, including surveys, interviews, artifact and evidence reviews, benchmarking, capability maturity modeling, and capability alignment with industry-recognized and industry-leading functional inventories.
12. The information security program functional inventory components include business operation risk and compliance, whereas the information risk management program functional inventory components include the chief information security officer (CISO) and enterprise resiliency.
13. Key indicators of business acceptance of ISRM include the time in the development cycle of products and services at which ISRM programs and capabilities are engaged and the number of policy exception requests that are applied for by the business and then granted by the ISRM organization.
14. Enterprise risk management (ERM) often has the maturity or knowledge to properly incorporate information risk into their assessment, ranking and reporting. Consequently, the ISRM program and capabilities do not need to work closely with the ERM organization or associated stakeholders to understand their needs or to assist them with their activities.
15. Some of the key industry standards (or good practices) with which ISRM organizations and capabilities may elect to demonstrate alignment include ISO 27001-27008 and 31000 and COBIT.

SATHIYAMURTHY ARTICLE

16. A proactive business model would embrace an agenda that recognizes the critical role information privacy plays in the successful realization of business objectives and would transition toward a holistic privacy management archetype.
17. The data custodian is responsible for ensuring that the data elements within the organization are in good health in terms of accuracy, completeness and consistency. The data steward enforces business rules on information, validates the security over information, approves access requests and maintains currency of access groups.
18. The IT privacy control layer safeguards the long-term best interest of the privacy program by establishing controls to address any control weaknesses and promote compliance with laws and industry-leading practices, governance portfolios, and risk management strategies. The key elements of the control layer include risk management, compliance, audit and assurance.

ISACA Journal

CPE Quiz

Based on Volume 2, 2011—Risk Management —What Is Your Capacity?

Quiz #137 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC# _____

Quiz #137

True or False

ROSS ARTICLE

1. _____
2. _____

SINGLETON ARTICLE

3. _____
4. _____
5. _____

JEGOUSSE ARTICLE

6. _____
7. _____

FISCHER ARTICLE

8. _____
9. _____
10. _____

PIRONTI ARTICLE

11. _____
12. _____
13. _____
14. _____
15. _____

SATHIYAMURTHY ARTICLE

16. _____
17. _____
18. _____

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current *Journal* subscribers. An electronic version of the quiz is available at *www.isaca.org/cpequiz*; it is graded online and is available to all interested parties.

If choosing to submit using this print copy, please e-mail, fax or mail your answers for grading. Return your answers and contact information by e-mail to *info@isaca.org* or by fax to +1.847.253.1443. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA.

Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

You will be responsible for submitting your credit hours at year-end for CPE credits.

A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.

Answers—Crossword by Myles Mellor

See page 49 for the puzzle.

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of IT audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards are a cornerstone of the ISACA professional contribution to the audit and assurance community. The framework for the IT Audit and Assurance Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance.
  They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework's concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, *www.isaca.org/cobit*.

Links to current guidance are posted on the standards page, *www.isaca.org/standards.*

The titles of issued standards documents are:

IT Audit and Assurance Standards
S1 Audit Charter Effective 1 January 2005
S2 Independence Effective 1 January 2005
S3 Professional Ethics and Standards Effective 1 January 2005
S4 Professional Competence Effective 1 January 2005
S5 Planning Effective 1 January 2005
S6 Performance of Audit Work Effective 1 January 2005
S7 Reporting Effective 1 January 2005
S8 Follow-up Activities Effective 1 January 2005
S9 Irregularities and Illegal Acts Effective 1 September 2005
S10 IT Governance Effective 1 September 2005
S11 Use of Risk Assessment in Audit Planning Effective 1 November 2005
S12 Audit Materiality Effective 1 July 2006
S13 Using the Work of Other Experts Effective 1 July 2006
S14 Audit Evidence Effective 1 July 2006
S15 IT Controls Effective 1 February 2008
S16 E-commerce Effective 1 February 2008

IT Audit and Assurance Guidelines
G1 Using the Work of Other Experts Effective 1 March 2008
G2 Audit Evidence Requirement Effective 1 May 2008
G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
G5 Audit Charter Effective 1 February 2008
G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
G7 Due Professional Care Effective 1 March 2008
G8 Audit Documentation Effective 1 March 2008
G9 Audit Considerations for Irregularities Effective 1 September 2008
G10 Audit Sampling Effective 1 August 2008
G11 Effect of Pervasive IS Controls Effective 1 August 2008
G12 Organisational Relationship and Independence Effective 1 August 2008
G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
G14 Application Systems Review Effective 1 October 2008
G15 Audit Planning Revised Effective 1 Ma1 2010
G16 Effect of Third Parties on an Organisation's IT Controls Effective 1 March 2009
G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 1 May 2010
G18 IT Governance Effective 1 May 2010
G19 Withdrawn 1 September 2008
G20 Reporting Effective Effective 16 September 2010
G21 Enterprise Resource Planning (ERP) Systems Review Effective 16 September 2010
G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
G24 Internet Banking Effective 1 August 2003
G25 Review of Virtual Private Networks Effective 1 July 2004
G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
G27 Mobile Computing Effective 1 September 2004
G28 Computer Forensics Effective 1 September 2004
G29 Post-implementation Review Effective 1 January 2005
G30 Competence Effective 1 June 2005
G31 Privacy Effective 1 June 2005
G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
G33 General Considerations for the Use of the Internet Effective 1 March 2006
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G36 Biometric Controls Effective 1 February 2007
G37 Configuration and Release Management Effective 1 November 2007
G38 Access Controls Effective 1 February 2008
G39 IT Organisation Effective 1 May 2008
G40 Review of Security Management Practices Effective 1 October 2008
G41 Return on Security Investment (ROSI) Effective 1 May 2010
G42 Continuous Assurance Effective 1 May 2010

IT Audit and Assurance Tools and Techniques
P1 IS Risk Assessment Measurement Effective 1 July 2002
P2 Digital Signatures and Key Management Effective 1 July 2002
P3 Intrusion Detection Systems (IDS) Review Effective 1 August 2003
P4 Malicious Logic Effective 1 August 2003
P5 Control Risk Self-assessment Effective 1 August 2003
P6 Firewalls Effective 1 August 2003
P7 Irregularities and Illegal Acts Effective 1 December 2003
P8 Security Assessment—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
P10 Business Application Change Control Effective 1 October 2005
P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

Standards for Information System Control Professionals Effective 1 September 1999
510 Statement of Scope
.010 Responsibility, Authority and Accountability
520 Independence
.010 Professional Independence
.020 Organisational Relationship
530 Professional Ethics and Standards
.010 Code of Professional Ethics
.020 Due Professional Care
540 Competence
.010 Skills and Knowledge
.020 Continuing Professional Education
550 Planning
.010 Control Planning
560 Performance of Work
.010 Supervision
.020 Evidence
.030 Effectiveness
570 Reporting
.010 Periodic Reporting
580 Follow-up Activities
.010 Follow-up

Code of Professional Ethics Effective 1 January 2011

Advertisers/Web Sites

ISACA® Journal, formerly *Information Systems Control Journal*, is published by ISACA, a nonprofit organization created for the public in 1969. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

Subscription Rates:
US: one year (6 issues) $75.00
All international orders: one year (6 issues) $90.00. Remittance must be made in US funds.

ISSN 1944-1967

Leaders and Supporters

ISACA®
Trust in, and value from, information systems

ISACA Bookstore

Resources for your Professional Development

Over 350 titles are available for sale through the ISACA® Bookstore. This insert highlights the new ISACA research and peer-reviewed books. See *www.isaca.org/bookstore* for the complete ISACA Bookstore listings.

2011 CISA® EXAM REFERENCE MATERIALS

See *www.isaca.org/cisabooks* to prepare for the December 2011 CISA exam.

CISA REVIEW MANUAL 2011

CRM-11 English Edition
CRM-11C Chinese Simplified Edition
CRM-11F French Edition
CRM-11I Italian Edition
CRM-11J Japanese Edition
CRM-11S Spanish Edition

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

QAE-11 English Edition (900 Questions)
QAE-11C Chinese Simplified Edition (900 Questions)
QAE-11G German Edition (900 Questions)
QAE-11I Italian Edition (900 Questions)
QAE-11J Japanese Edition (900 Questions)
QAE-11S Spanish Edition (900 Questions)

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011 SUPPLEMENT

QAE-11ES English Edition (100 Questions)
QAE-11CS Chinese Simplified Edition (100 Questions)
QAE-11FS French Edition (100 Questions)
QAE-11GS German Edition (100 Questions)
QAE-11IS Italian Edition (100 Questions)
QAE-11JS Japanese Edition (100 Questions)
QAE-11SS Spanish Edition (100 Questions)

CISA PRACTICE QUESTION DATABASE V11

(1,000 Questions)
CDB-11 CD-ROM—English Edition
CDB-11W Download—English Edition (no shipping charges apply to download)
CDB-11S CD-ROM—Spanish Edition
CDB-11SW Download—Spanish Edition (no shipping charges apply to download)

CANDIDATE'S GUIDE TO THE CISA EXAM AND CERTIFICATION

CAN (No charge to paid CISA exam registrants)

2011 CISM® EXAM REFERENCE MATERIALS

See *www.isaca.org/cismbooks* to prepare for the December 2011 CISM exam.

CISM REVIEW MANUAL 2011

CM-11 English Edition
CM-11J Japanese Edition
CM-11S Spanish Edition

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CQA-11 English Edition (650 Questions)
CQA-11J Japanese Edition (650 Questions)
CQA-11S Spanish Edition (650 Questions)

CISM REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011 SUPPLEMENT

CQA-11ES English Edition (100 Questions)
CQA-11JS Japanese Edition (100 Questions)
CQA-11SS Spanish Edition (100 Questions)

CISM PRACTICE QUESTION DATABASE V11

(750 Questions)
MDB-11 CD-ROM – English Edition
MDB-11W Download – English Edition (no shipping charges apply to download)

CANDIDATE'S GUIDE TO THE CISM EXAM AND CERTIFICATION

CGC (No charge to paid CISM exam registrants)

2011 CGEIT EXAM REFERENCE MATERIALS

See *www.isaca.org/cgeitbooks* to prepare for the December 2011 CGEIT exam.

CGEIT REVIEW MANUAL 2011

CGM-11 English Edition

CGEIT REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CGQ-11 English Edition (60 Questions)

CANDIDATE'S GUIDE TO THE CGEIT EXAM AND CERTIFICATION

CACG (No charge to paid CGEIT exam registrants)

2011 CRISC EXAM REFERENCE MATERIALS

See *www.isaca.org/criscbooks* to prepare for the December 2011 CISA exam.

CRISC REVIEW MANUAL 2011

CRR-11 English Edition

CRISC REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL 2011

CRQ-11 English Edition (100 Questions)

CANDIDATE'S GUIDE TO THE CRISC EXAM AND CERTIFICATION

CACR (No charge to paid CRISC exam registrants)

COBIT®

See *www.isaca.org/cobitbooks* for complete descriptions and additional titles.

COBIT® 4.1

IT Governance Institute

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT was first published by ITGI in April 1996. ITGI's latest update—COBIT® 4.1—emphasizes regulatory compliance, helps organizations to increase the value attained from IT, highlights links between business and IT goals, and simplifies implementation of the COBIT framework. COBIT 4.1 is a fine-tuning of the COBIT framework and can be used to enhance work already done based upon earlier versions of COBIT. When major activities are planned for IT governance initiatives, or when an overhaul of the enterprise control framework is anticipated, it is recommended to start fresh with COBIT 4.1. COBIT 4.1 presents activities in a more streamlined and practical manner so continuous improvement in IT governance is easier than ever to achieve. 2007, 196 pages. **CB4.1**

COBIT AND APPLICATION CONTROLS: A MANAGEMENT GUIDE

ISACA

COBIT and Application Controls is structured based on the life cycle of application systems—from defining requirements through providing assurance on application controls. The concepts presented apply to new and existing legacy application systems. The book also offers guidance on:

- The definition and nature of application controls (addressing the six application controls discussed in COBIT)
- The design and operation of application controls
- Relationships and dependencies that application controls have with other controls, such as IT general controls
- The responsibilities of business and IT management

This guide helps business executives, business and IT managers, IT developers and implementers, and internal and external auditors implement, manage and provide assurance regarding application controls. 2009, 101 pages. **CAC**

COBIT SECURITY BASELINE, 2ND EDITION

IT Governance Institute

This publication focuses on IT security risk in a way that is simple to follow and implement for everyone, from the home user or small-to medium-sized enterprise to executives and board members of larger organizations. *COBIT® Security Baseline* provides an introduction to information security; an explanation of why security is important; the COBIT-based security baseline, mapped to ISO/IEC 27002; information security "survival kits" for varying audiences; and a summary of technical security risks. 2007, 48 pages. **CBSB2**

COBIT CONTROL PRACTICES: GUIDANCE TO ACHIEVE CONTROL OBJECTIVES FOR SUCCESSFUL IT GOVERNANCE, 2ND EDITION

IT Governance Institute

Control practices are derived from each control objective and help management, service providers, end users and control professionals to justify and design the specific controls needed to improve IT governance. The control practices provide the how, why and what to implement for each control objective, to improve IT performance and/or address IT solution and service delivery risks. By providing guidance on why controls are needed and what the best practices are for meeting specific control objectives, *COBIT® Control Practices* helps ensure that solutions put forward are likely to be more completely and successfully implemented. *COBIT® Control Practices* presents the key control mechanisms that support the achievement of control objectives. 2007, 174 pages. **CPS2**

COBIT QUICKSTART, 2nd EDITION

IT Governance Institute

COBIT® Quickstart is specifically designed to assist in rapid and easy adoption of the most essential elements of COBIT. *Quickstart* is a summarized version of the COBIT resources, focusing on the most crucial IT processes, control objectives and metrics, all presented in an easy-to-follow format to help users gain the benefits of COBIT quickly. *Quickstart* was designed as a baseline for many small to medium enterprises, but is also suitable for large organizations as a tool to accelerate adoption of IT governance best practices. *Quickstart* will help you to rapidly understand the important issues and management priorities. It can be followed by nontechnical people or managers who want principles, not detail, and is a useful springboard to the more comprehensive COBIT guidance. 2007, 58 pages. **CBQ2**

COBIT USER GUIDE FOR SERVICE MANAGERS

IT Governance Institute

This is the first of a planned series aimed at providing specific guidance on how to use COBIT when performing a particular role. The first publication is focused on the service manager, as it is known that this is a significant role where there is a high demand for guidance. Each guide will highlight a specific group of COBIT users and describe how to use COBIT to support their activities, how to focus on the parts of COBIT that are most relevant to them, and how COBIT relates to the best practices and standards that they would typically use in their job. This guide contains an introduction to the business and governance challenges facing service managers and describes how COBIT can help, an explanation of the service manager role and why it is important for effective IT governance, the key governance tasks for the role aligned with the ITIL V3 processes and COBIT 4.1 control objectives, case examples, a high level maturity model for the role area, and links to other references. 2009, 54 pages. **CUG**

IMPLEMENTING AND CONTINUALLY IMPROVING IT GOVERNANCE

ISACA

Replacing the popular *IT Governance Implementation Guide*, this publication assists enterprises in establishing and sustaining an effective approach to governing IT.

New features include Risk IT-related content as well as typical pain points that new or improved IT governance practices can help solve, including outsourcing service delivery problems and business frustration with failed initiatives.

Implementing and Continually Improving IT Governance is based on a life cycle of continuous improvement. In addition to describing the steps that need to be considered and undertaken to progress an IT governance initiative, this guide identifies trigger events that indicate the need for better governance, as well as implementation challenges enterprises might face. It also describes how to use COBIT, Val IT and Risk IT components for critical support. 2009, 78 pages. **ITG9**

IT ASSURANCE GUIDE: USING COBIT

IT Governance Institute

Management needs assurance that the desired IT goals and objectives are being met and that key controls are in place and effective. The *IT Assurance Guide* introduces the various types of IT assurance activities that exist and describes how COBIT can be used to support such activities. It provides invaluable guidance for assurance professionals and a structured assurance approach linked to the COBIT framework that provides a common language and criteria for business and IT people. This approach facilitates a shared identification of control priorities and improvements.
2007, 269 pages. **CB4A**

SHAREPOINT DEPLOYMENT AND GOVERNANCE USING COBIT 4.1: A PRACTICAL APPROACH

Dave Chennault and Chuck Strain

SharePoint has quickly become one of Microsoft's most successful products and the *de facto* collaboration standard. But deployment is often accompanied by chaos and a wave of frustration called "the SharePoint Effect" as organizations become overwhelmed by their own success, a lack of planning or insufficient governance. While many bloggers and self-appointed experts have offered "best practice" guidelines, *SharePoint Deployment and Governance Using COBIT 4.1* contains a comprehensive, step-by-step guide on how to practically deploy and govern SharePoint 2007 and 2010 using COBIT 4.1, the leading internationally accepted governance framework.

This practical guide blends the needs of the deployment staff and audit teams with a comprehensive blueprint that puts business in charge. The book is filled with authoritative tips, techniques and advice on:

- How to use COBIT 4.1 for SharePoint deployment and governance—on premises or in the cloud
- Specific considerations when using SharePoint 2007 or SharePoint 2010
- Which third-party tools to consider to govern your SharePoint farm
- How to apply appropriate COBIT processes at each stage of the SharePoint deployment

2010, 176 pages. **SDG**

RISK IT AND RISK RELATED TOPICS

See *www.isaca.org/riskitbooks* for additional information.

THE RISK IT FRAMEWORK
ISACA

The Risk IT Framework provides a set of guiding principles and supporting practices for enterprise management, combined to deliver a comprehensive process model for governing and managing IT risk. For users of COBIT and Val IT, this process model will look familiar. Guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of each process. The model is divided into three domains—Risk Governance, Risk Evaluation, Risk Response—each containing three processes:
- Risk Governance
- Risk Evaluation
- Risk Response

2009, 104 pages. **RITF**

THE RISK IT PRACTITIONER GUIDE
ISACA

The Risk IT Practitioner Guide, a support document for the Risk IT framework, provides examples of possible techniques to address IT-related risk issues, and more detailed guidance on how to approach the concepts covered in the process model.

Concepts and techniques explored in more detail include:
- Building enterprise-specific scenarios, based on a set of generic IT risk scenarios
- Building a risk map, using techniques to describe the impact and frequency of scenarios
- Building impact criteria with business relevance
- Defining key risk indicators (KRIs)
- Using COBIT and Val IT to mitigate risk; the link between risk and COBIT control objectives and Val IT key management practices

2009, 134 pages. **RITPG**

Val IT™

See *www.isaca.org/valitbooks* for complete descriptions.

THE VAL IT FRAMEWORK 2.0
ISACA

This publication is the foundation document in the Val IT series. It presents practices for three domains:
- Value Governance
- Portfolio Management
- Investment Management

Each of these domains is broken down into key management processes and a number of key management practices.

This edition simplifies the management processes and practices, and extends the Val IT Framework beyond new investments to include IT services, assets and other resources. It also aligns terminology with COBIT, and adds a management guidelines section, similar to COBIT, which provides a greater level of detail on the Val IT processes, key management practices and maturity models for each Val IT domain. 2008, 146 pages. **VITF2**

GETTING STARTED WITH VALUE MANAGEMENT
ISACA

This is a guide that outlines "how to implement" Val IT and compliments the *The Val IT Framework,* which describes "what you do." *Getting Started With Value Management* is made up of six chapters that flow in a logical sequence moving from typical starting points, pain points or "trigger points" to specific approaches to address these points.

It offers assessment templates and practical guidance on how to use the new framework, along with recommended approaches to addressing investment issues in organizations. It contains suggested maturity models and approaches to maintaining and sustaining change. 2008, 44 pages. **VITM**

VALUE MANAGEMENT GUIDANCE FOR ASSURANCE PROFESSIONALS—USING VAL IT 2.0
ISACA

The objective of the newest publication to the Val IT family *Value Management Guidance for Assurance Professionals—Using Val IT 2.0* is to provide guidance on how to use Val IT to support an assurance review focused on the governance of IT-enabled business investments for each of the three Val IT domains—Value Governance, Portfolio Management and Investment Management. This guide is based on the *IT Assurance Guide Using COBIT* which provides comprehensive guidance on planning and performing a wide range of IT related assurance activities. This guide is focused on an assurance review of IT value management based on and aligned with the *Val IT 2.0 Framework*—the governance of IT related business investments. Readers should be familiar with Val IT 2.0. Readers wishing to obtain a fuller description and understanding of IT assurance principles and context should refer to the *IT Assurance Guide: Using COBIT.* 2010, 48 pages. **VITAG**

THE BUSINESS CASE GUIDE—USING VAL IT 2.0
ISACA

The intention of this publication is to position the business case as a valuable management tool—an operational tool—and to provide an easy-to-follow guide, based on Val IT 2.0, to creating, maintaining and using the business case. As such, this publication builds on and enhances the earlier version of this guide, *Enterprise Value: Governance of IT Investments, The Business Case* (2006). This new publication is now fully aligned with Val IT 2.0, provides "how to do it" tips, maturity models, examples and references to other materials for using and implementing the business case processes as the powerful operational tools they have the potential to be. 2010, 49 pages. **VITB2**

AUDIT, CONTROL AND SECURITY—ESSENTIALS

See *www.isaca.org/essentialsbooks* for complete descriptions and additional essential titles.

ACCESS CONTROL, SECURITY, AND TRUST: A LOGICAL APPROACH
NEW

Shiu-Kai Chin and Susan Beth Older

Access Control, Security, and Trust: A Logical Approach equips readers with an access control logic that they can use to specify and verify their security designs. Throughout the text, the authors use a single access control logic based on a simple propositional modal logic. The first part of the book presents the syntax and semantics of access control logic, basic access control concepts, and an introduction to confidentiality and integrity policies. The second section covers access control in networks, delegation, protocols and the use of cryptography. In the third section, the authors focus on hardware and virtual machines. The final part discusses confidentiality, integrity and role-based access control. Taking a logical, rigorous approach to access control, this book shows how logic is a useful tool for analyzing security designs and spelling out the conditions upon which access control decisions depend. 2010, 351 pages. **48-CRC**

IT AUDITING USING CONTROLS TO PROTECT INFORMATION ASSETS, 2ND EDITION
NEW EDITION

Chris Davis, Mike Schiller, Kevin Wheeler

Filled with solid techniques, checklists, forms, coverage of leading-edge tools and systematic procedures for common IT audits, *IT Auditing, 2nd Edition* covers real-life scenarios and fosters the skills necessary for auditing complex IT systems. Fully updated to cover new technology including cloud computing, virtualization and storage, the book provides guidance on creating an effective and value-added internal IT audit function. Information is presented in easy-to-follow sections, allowing you to quickly grasp critical and practical techniques.

This edition contains updated tools and checklists, as well as discussions of key concepts and methods for their effective use. This definitive guide offers a unique combination of how-to information on IT auditing for new auditors and cutting-edge audit techniques for experienced professionals. 2011, 512 pages. **15-MIT2**

ITAF: A PROFESSIONAL PRACTICES FRAMEWORK FOR IT ASSURANCE
ISACA

ITAF: A Professional Practices Framework for IT Assurance consists of compliance and good practice setting guidance. The IT Assurance Framework™ (ITAF™):
- Provides direction on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge, skills and diligence, conduct, and reporting requirements

ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports. 2008, 71 pages. **WITAF**

IT SECURITY METRICS: A PRACTICAL FRAMEWORK FOR MEASURING SECURITY & PROTECTING DATA
NEW

Lance Hayden

IT Security Metrics provides a comprehensive approach to measuring risks, threats, operational activities and the effectiveness of data protection in your organization. The book explains how to choose and design effective measurement strategies and addresses the data requirements of those strategies. The Security Process Management Framework is introduced and analytical strategies for security metrics data are discussed. Readers are shown how to take a security metrics program and adapt it to a variety of organizational contexts to achieve continuous security improvement over time. Real-world examples of security measurement projects are included in this definitive guide. 2010, 396 pages. **22-MSM**

IT STRATEGIC AND OPERATIONAL CONTROLS
NEW

John Kyriazoglou

Nowadays, integrated information systems can significantly magnify the accrued benefits of a given project and greatly strengthen an organization, but such benefits are balanced by a serious risk. If IT systems are not used in a disciplined manner, they can create havoc and frequently bring about unexpected results and catastrophe, as shown by the rise in security incidents and computer-based crimes.

Written with practicality and convenience in mind, this book is an ideal tool for those without specialized technical expertise who are seeking to understand IT controls and their design, implementation, monitoring, review and audit issues. This book provides a comprehensive guide to implementing an integrated and flexible set of IT controls in a systematic way. It can help organizations to formulate a complete culture for all areas that must be supervised and controlled—allowing them to simultaneously ensure a secure, high standard whilst striving to obtain the strategic and operational goals of the company. 2010, 686 pages. **6-ITSOC**

A NEW AUDITOR'S GUIDE TO PLANNING, PERFORMING, AND PRESENTING IT AUDITS
NEW

Nelson Gibbs, Divakar Jain, Amitesh Joshi, Surekha Muddamsetti, Sarabjot Singh

Information technology is a highly dynamic, rapidly changing environment. IT auditors are expected to stay current with the latest tools, technologies, and trends, and may need to do additional research to prepare for specific audits. This book is designed to help aspiring and active internal auditors take a step back and understand the general process and activities involved in conducting an audit around technology.

This book uses a simplified four-layer technology model of networks, operating systems, databases, and applications. It provides easily understandable concepts of the technology environment that can be applied in most organizations with little modification. 2010, 225 pages. **1-II**

SAP SECURITY AND RISK MANAGEMENT, 2ND EDITION
NEW

Mario Linkies and Horst Karin

The revised and expanded second edition of this best-selling book describes all requirements, basic principles and best practices of security for an SAP system. Readers will learn how to protect each SAP component internally and externally while also complying with legal requirements. Furthermore, the book describes how to master the interaction of these requirements to provide a holistic security and risk management solution. Using numerous examples and step-by-step instructions, this book teaches the reader the technical details of implementing security in SAP NetWeaver. 2010, 726 pages. **2-SAPP**

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

See *www.isaca.org/specificbooks* for complete descriptions and additional specific environment titles.

FRAUD AUDITING AND FORENSIC ACCOUNTING, 4TH EDITION
NEW

Tommie W. Singleton, Aaron J. Singleton

With the responsibility of detecting and preventing fraud falling heavily on the accounting profession, every accountant needs to recognize fraud and learn the tools and strategies necessary to catch it in time. Providing valuable information to those responsible for dealing with prevention and discovery of financial deception, *Fraud Auditing and Forensic Accounting, 4th Edition* helps accountants develop an investigative eye toward both internal and external fraud and provides tips for coping with fraud when it is found to have occurred.

This book includes step-by-step keys to fraud investigation and the most current methods for dealing with financial fraud within the organization. Written by recognized experts in the field of white-collar crime, this fourth edition provides readers, whether beginning forensic accountants or experienced investigators, with industry-tested methods for detecting, investigating and preventing financial schemes. 2010, 317 pages. **88-WFA**

IDENTITY MANAGEMENT: CONCEPTS, TECHNOLOGIES, AND SYSTEMS
NEW

Elisa Bertino, Kenji Takahashi

Digital identity can be defined as the digital representation of the information known about a specific individual or organization. Digital identity management technology is an essential function in customizing and enhancing the network user experience, protecting privacy, underpinning accountability in transactions and interactions, and complying with regulatory controls. This practical resource offers readers an in-depth understanding of how to design, deploy and assess identity management solutions. It provides a comprehensive overview of current trends and future directions in identity management, including best practices, the standardization landscape and the latest research finding. Additionally, readers are given a clear explanation of fundamental notions and techniques that cover the entire identity life cycle. 2011, 194 pages. **10-ART**

ISACA member complimentary PDF *www.isaca.org/downloads*

PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS

NEW

Joe Weiss

Aimed at both the novice and expert in IT security and industrial control systems (ICS), this book will help readers gain a better understanding of protecting ICSs from electronic threats. Cybersecurity is getting much more attention and SCADA security (supervisory control and data acquisition) is a particularly important part of this field, as are distributed control systems (DCS), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), and all other field controllers, sensors, drives and emission controls that make up the "intelligence" of modern industrial buildings and facilities. 2010, 327 pages. **1-MPPI**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE® E-BUSINESS SUITE, 3RD EDITION

ISACA

This updated edition of one of ISACA's most popular guides reflects the many changes that the business environment and Oracle ERP application have undergone since the second edition was published. In response to customer needs and an increased market awareness of governance, risk and compliance (GRC), Oracle Corporation has continued to boost its GRC offerings and released the updated and improved Oracle E-Business Suite R12.1 (EBS) in 2009.

This in-demand guide also provides an update on current industry standards and identifies future trends in Oracle EBS risk and control. It enables audit, assurance, risk and security professionals (IT and non-IT) to evaluate risks and controls in existing ERP implementations, and facilitate the design and implementation of better practice controls into system upgrades and enhancements. This book also aims to assist system architects, business analysts and business process owners who are implementing Oracle EBS, as well as people responsible for managing it in live production to maintain the appropriate level of control and security according to business needs and industry standards. 2010, 407 pages. **ISOA3**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE® DATABASE, 3RD EDITION

ISACA

Security, Audit and Control Features Oracle Database, 3rd Edition, provides a new perspective of security and controls over Oracle. This updated edition includes a background and review of security controls and addresses the risks associated with protecting information in a distributed computing environment of various platforms, versions, interfaces and tools.

The goal of this popular book is to guide the assessor through a comprehensive evaluation of security for an Oracle database based on business objectives and risks. It examines several different frameworks that can be used to assess security risks and covers technical topics, including an overview of Oracle Database's architecture, operating system controls, auditing and logging, network security, and new features in Oracle 11*g* (differences from previous versions of Oracle Database are noted, as well as differences that may exist based on the host operating system of the database).

Security, Audit and Control Features Oracle® Database helps simplify a daunting task, giving readers the approach, knowledge and tools to effectively plan and execute an Oracle Database security assessment. 2009, 219 pages. **ODB9**

SECURITY, AUDIT AND CONTROL FEATURES SAP® ERP: TECHNICAL AND RISK MANAGEMENT REFERENCE SERIES, 3RD EDITION

Deloitte Touche Tohmatsu Research Team and ISACA

Security, Audit and Control Features SAP® ERP, 3rd Edition, part of the Technical and Risk Management Reference Series, enables assurance, security and risk professionals to evaluate risks and controls in existing ERP implementations and facilitates the design and building of controls into system upgrades and enhancements.

The publication is based on SAP ERP (also known as SAP ERP Central Component [ECC]), the latest version of which is SAP ECC 6.0.

This in-demand new edition has been updated to reflect:
- New/modified SAP transaction codes and reports
- SAP ERP based on a service-oriented architecture (SOA). SOA combines SAP ERP with an open technology platform that can integrate SAP and non-SAP systems using the SAP Netweaver platform.
- SAP GRC suite of tools, including Access Control and Process Control, which offers corporate governance and risk management solutions

2009, 470 pages. **ISAP3**

NON-ENGLISH RESOURCES

See *www.isaca.org/nonenglishbooks*
for complete descriptions and additional non-English titles.

ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN

Manuel Tupia Anticona

2010, 201 págs. **2-TCA**

AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.

Piattini, M. y otros

2008, 732 págs. **3-RAMA**

CISA EXAMINATION REFERENCE MATERIAL

Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the December 2011 CISA exam—see page S5

CISM EXAMINATION REFERENCE MATERIAL

Study aids available in Japanese and Spanish for the December 2011 CISM exam—see page S5

COMPUTACIÓN FORENSE: DESCUBRIENDO LOS RASTROS INFORMÁTICOS

Jeimy Cano

2009, 340 págs. **1-AOCF**

PRINCIPIOS DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACIÓN

Manuel Tupia Anticona

2009, 204 págs. **1-TCA**

SECURITY, AUDIT AND CONTROL FEATURES ORACLE E-BUSINESS SUITE: A TECHNICAL AND RISK MANAGEMENT REFERENCE GUIDE

Japanese Edition. 2006, 368 pages. **ISOAJ**

SECURITY, AUDIT AND CONTROL FEATURES SAP R/3: A TECHNICAL AND RISK MANAGEMENT REFERENCE GUIDE

Japanese Edition. 2006, 255 pages. **ISAPJ**

INTERNET AND RELATED SECURITY TOPICS

See *www.isaca.org/internetbooks*
for complete descriptions and additional Internet and related security titles.

CLOUD COMPUTING: IMPLEMENTATION, MANAGEMENT, AND SECURITY

John W. Rittinghouse and James F. Ransome

This guide provides an understanding of what cloud computing really means, explores how disruptive it may become in the future, and examines its advantages and disadvantages. It gives business executives the knowledge necessary to make informed, educated decisions regarding cloud initiatives. The authors first discuss the evolution of computing from a historical perspective, focusing primarily on advances that led to the development of cloud computing. They then survey some of the critical components that are necessary to make the cloud computing paradigm feasible. They also present various standards based on the use and implementation issues surrounding cloud computing and describe the infrastructure management that is maintained by cloud computing service providers. After addressing significant legal and philosophical issues, the book concludes with a hard look at successful cloud computing vendors.

Helping to overcome the lack of understanding currently preventing even faster adoption of cloud computing, this book arms readers with guidance essential to make smart, strategic decisions on cloud initiatives. 2009, 340 pages. **45-CRC**

CYBER ATTACKS: PROTECTING NATIONAL INFRASTRUCTURE

NEW

Edward Amoroso

No nation has a coherent technical and architectural strategy for preventing cyber attacks from crippling essential critical infrastructure services. This book initiates an intelligent national and international dialogue amongst the general technical community around proper methods for reducing national risk. This includes controversial themes such as the deliberate use of deception to trap intruders. It also serves as an attractive framework for a new national strategy for cyber security, something that several administrations have failed in attempting to create. This book offers a technical, architectural, and management solution to the problem of protecting national infrastructure. It takes the debate on protecting critical infrastructure in an entirely new and fruitful direction. 2011, 248 pages. **11-EL**

CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS

NEW

Sumit Ghosh, Elliot Turrini (Editors)

Designed to serve as a reference work for practitioners, academics and scholars worldwide, this book is the first of its kind to explain complex cybercrimes from the perspectives of multiple disciplines and to scientifically analyze their impact on individuals, society and nations, holistically and comprehensively. In particular, the books shows how multiple disciplines concurrently bring out the complex, subtle, and elusive nature of cybercrimes; how conventional laws and traditional thinking fall short in protecting organizations from cybercrimes; and how to transform the destructive potential of cybercrimes into amazing innovations in cyberspace that can lead to explosive technological growth and prosperity. 2011, 414 pages. **2-SCC**

GRAY HAT HACKING: THE ETHICAL HACKERS HANDBOOK, 3RD EDITION

Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams

Featuring in-depth, advanced coverage of vulnerability discovery and reverse engineering, *Gray Hat Hacking, 3rd Edition* provides eight brand-new chapters on the latest ethical hacking techniques. In addition to the new chapters, the rest of the book is updated to address current issues, threats, tools and techniques.

This one-of-a-kind guide offers a comprehensive overview of the hacking landscape and is organized in a progressive manner, first giving an update on the latest developments in hacking-related law, useful to everyone in the security field. Next, the book describes the security testing process and covers useful tools and exploit frameworks. The second section is expanded by explaining social engineering, physical and insider attacks, and the latest trends in hacking (voice over-IP and SCADA attacks). The book then explains, from both a code and machine-level perspective, how exploits work and guides readers through writing simple exploits. Finally, the authors provide a comprehensive description of vulnerability research and reverse engineering. 2011, 720 pages. **4-MGH3**

HACKING EXPOSED WEB APPLICATIONS, 3RD EDITION

NEW

Joel Scambray

Protect your web applications from malicious attacks by mastering the weapons and thought processes of today's hacker. Written by recognized security practitioners and thought leaders, *Hacking Exposed Web Applications, 3rd Edition* is fully updated to cover new infiltration methods and countermeasures. Find out how to reinforce authentication and authorization, plug holes in Firefox and IE, reinforce against injection attacks, and secure web 2.0 features. Integrating security into the web development lifecycle and into the broader enterprise information security program is also covered in this comprehensive resource. 2010, 482 pages. **23-MHE**

MOBILE APPLICATION SECURITY

Himanshu Dwivedi, Chris Clark, David Thiel

Implement a systematic approach to security in mobile application development with help from this practical guide. Featuring case studies, code examples and best practices, *Mobile Application Security* details how to protect against vulnerabilities in the latest smartphone and PDA platforms. Maximize isolation, lockdown internal and removable storage, work with sandboxing and signing, and encrypt sensitive user information. Safeguards against viruses, worms, malware and buffer overflow exploits are also covered in this comprehensive resource. 2010, 432 pages. **21-MMS**

NO ROOT FOR YOU: A SERIES OF TUTORIALS, RANTS AND RAVES, AND OTHER RANDOM NUANCES THEREIN

NEW

Gordon L. Johnson

Over the years, spoon-fed information on anything that involves network auditing has been rather scarce. This book intends to meet this need, proving that such tasks may be explained in an articulate manner, while still maintaining a proper rapport with the individual. This book speaks in layman's terms, while still maintaining proper terminology and utilizing metaphors to express the idea in a more understandable form. A quick-reference for network auditors, it contains step-by-step, illustrated tutorials, explanations regarding why each exploitation works, and information on how to defend against such attacks. 2008, 424 pages. **1-WCNR**

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IMPLEMENTATION

NEW

David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask

Written by IT security experts, *Security Information and Event Management (SIEM) Implementation* shows the reader how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. Readers will also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource.
2010, 464 pages. **24-MSIEM**

SYSTEM FORENSICS, INVESTIGATION, AND RESPONSE

NEW

John R. Vacca, K Rudolph

Computer crimes call for forensics specialists, people who know how to find and follow the evidence. *System Forensics, Investigation, and Response* begins by examining the fundamentals of system forensics, such as what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. The book then addresses the tools, techniques, and methods used to perform computer forensics and investigation. Finally, it explores emerging technologies as well as future directions of this interesting and cutting-edge field. 2011, 339 pages. **2-JBSF**

IT GOVERNANCE AND BUSINESS MANAGEMENT

See *www.isaca.org/managementbooks* for complete descriptions and additional IT governance and management titles.

THE BUSINESS MODEL FOR INFORMATION SECURITY

ISACA

The Business Model for Information Security provides an in-depth explanation to a holistic business model that examines security issues from a systems perspective. Explore various media, including journal articles, webcasts and podcasts, to delve into the Business Model for Information Security™ and to learn more about how to have success in the information security field in today's market.

The Business Model for Information Security enables security professionals to examine security from a systems perspective, creating an environment where security can be managed holistically and allowing actual risks to be addressed. 2010, 72 pages. **BMIS**

CREATING A CULTURE OF SECURITY (E-BOOK)

NEW

Steven J. Ross, Risk Masters and ISACA

No security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted. Therefore, if stakeholders are not grounded in a culture of security, there is potential for improper actions. The culture determines what an enterprise actually does about security (or any other objective) and not what it intends to do. An effective security culture supports the protection of information while also supporting the broader aims of the enterprise. To sustain a security culture, it is critical to understand whether it was created in a purposeful manner or by accident. A culture of security is not an end in itself, but a pathway to achieve and maintain other objectives, such as proper use of information. The greatest benefit to a culture of security is the effect it has on other dynamic interconnections within an enterprise. It leads to greater internal and external trust, consistency of results, easier compliance with laws and regulations and greater value in the enterprise as whole.

Creating a Culture of Security by Steven J. Ross, Risk Masters discusses how to achieve a meaningful, intentional security culture. It provides information on the benefits of, and inhibitors to, a culture of security. It discusses positive and negative reinforcement strategies and the steps to take to achieve the right balance in a security culture program. 2011, 140 pages. **WCCS**

CIO BEST PRACTICES: ENABLING STRATEGIC VALUE WITH INFORMATION TECHNOLOGY, 2ND EDITION

Joseph P. Stenzel, Gary Cokins, Karl D. Schubert, Michael H. Hugos

Anyone working in information technology feels the opportunities for creating and enabling lasting value. The chief information officer CIO helps define those opportunities and turn them into realities. Now in a second edition, *CIO Best Practices* is an essential guide offering real-world practices used by CIOs and other IT specialists who have successfully mastered the blend of business and IT responsibilities. For anyone who wants to achieve better returns on their IT investments, *CIO Best Practices, 2nd Edition* presents the leadership skills and competencies required of a CIO addressing comprehensive enterprise strategic frameworks to fully leverage IT resources.

This practical resource provides best practice guidance on the key responsibilities of CIOs and their indispensable executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important collection of best practices for achieving and exercising strategic IT leadership for CIOs, those who intend to become CIOs and those who want to understand the strategic importance of IT for the entire enterprise. 2010, 360 pages. **54-WCIO2**

EMPOWERING GREEN INITIATIVES WITH IT: A STRATEGY AND IMPLEMENTATION GUIDE

NEW

Carl H. Speshock

A straightforward guide to the role of IT departments and vendor's in assisting organizations in going green with the aid of IT-related resources and offerings. This book provides organizations with strategy, planning, implementation and, assessment guidance for their green initiatives. It discusses the many benefits of green initiatives with the assistance, integration and collaboration of the IT department and vendors, i.e., custom and vendor application development and reporting tools, green IT examples and, business intelligence dashboards that can perform analytical and predictive analysis of green related business data. Practical and thorough, this book includes helpful checklists, a glossary and resources to get started with a business's green initiatives. 2010, 235 pages. **89-WEG**

GREEN IT IN PRACTICE, 2ND EDITION

NEW

Gary Hird

This best-selling practical book helps managers to navigate the confusing mass of information surrounding Green IT with greater ease. Focusing on the experience of implementing the John Lewis Partnership's Green IT program, it contains a host of valuable ideas for establishing and formalizing a green IT initiative. Benefits of the book include:

- Understand the link between general corporate social responsibility and green IT
- Finding out how best to construct appropriate policies and metrics
- Practical tried and tested tips on how to engage with employees and suppliers
- An insight into other people's experiences through in-depth case studies
- A deeper appreciation of just how IT can begin to enable carbon footprint reduction in an organization as a whole

2010, 128 pages. **7-ITGR**

IMPLEMENTING THE PROJECT MANAGEMENT BALANCED SCORECARD

NEW

Jessica Keyes

Business managers have long known the power of the balanced scorecard in executing corporate strategy. *Implementing the Project Management Balanced Scorecard* shows project managers how they too can use this framework to meet strategic objectives. It supplies valuable insight into the project management process as a whole and contains detailed explanations on how to effectively implement the balanced scorecard to measure and manage performance and projects.

Filled with examples and case histories, the book directly relates the scorecard concept to the major project management steps of determining scope, scheduling, estimation, risk management, procurement and project termination. Complete with a plethora of resources in its appendices and on the accompanying CD, the text includes detailed instructions for developing a measurement program, a full metrics guide, a sample project plan and a set of project management fill-in forms. 2010, 447 pages, **46-CRC**

IT GOVERNANCE: A POCKET GUIDE

NEW

Alan Calder

This pocket guide outlines the key drivers for IT governance in the modern global economy, with particular reference to corporate governance requirements and the need for companies to protect their information assets. The guide examines the role of IT governance in the management of strategic and operational risk. It also looks at the most important considerations when setting up an IT governance framework, and introduces the reader to the Calder-Moir IT Governance Framework, which the author helped to create. The approach throughout avoids technical jargon and emphasizes business opportunities and needs. 2007, 52 pages. **4-ITIG**

IT GOVERNANCE: POLICIES & PROCEDURES, 2011 EDITION

NEW

Michael Wallace, Larry Webber

IT Governance Policies & Procedures will help you to devise an information systems policy and procedure program uniquely tailored to the needs of the reader's organization. Not only does it provide sample policies, but this valuable resource provides the information needed to develop useful and effective policies for your unique environment. For fingertip access to the information you need on policy and planning, documentation, systems analysis and design, and much more, the materials in this ready-reference desk manual can be used as models or templates to create similar documents for the reader's own organization. CD-ROM included. 2010, 981 pages. **5-AS11**

IT PROJECT MANAGEMENT: ON TRACK FROM START TO FINISH, 3RD EDITION

NEW

Joseph Phillips

This practical, up-to-date guide explains how to successfully manage an IT project and prepare for CompTIA Project+ certification. *IT Project Management: On Track from Start to Finish, 3rd Edition* walks you through each step of the IT project management process, covering critical strategies for on-time and within-budget projects. You'll get proven methods for initiating a project, selecting qualified team members, conferring with management, establishing communication, setting realistic timetables, tracking costs, and closing a project. CD-ROM included. 2010, 640 pages. **25-MIPM**

IT SERVICE MANAGEMENT: IMPLEMENTATION AND OPERATION

NEW

Ahmad K. Shuja

IT Service Management: Implementation and Operation focuses on how to achieve the best return from an IT service management implementation investment, in the least possible time. It discusses the key challenges organizations experience as they leverage ITIL Version 3 to achieve desired transformations and includes the approaches adopted to address those challenges. It includes templates, checklists, implementation patterns and detailed plans for each pattern to kick start implementation efforts.

Detailing the components needed to implement, operate and optimize ITIL service management, the text explains the organizational architecture required to achieve business-IT integration within ITIL. Complete with case studies, examples, problems and access to additional resources on the author's web site, the book illustrates how to achieve service management excellence with ITIL in a way that is seamless to customers and enables the delivery of business value effectively, visibly and efficiently. 2010, 554 pages. **47-CRC**

MONITORING INTERNAL CONTROL SYSTEMS AND IT

ISACA

Monitoring Internal Control Systems and IT provides useful guidance and tools for enterprises interested in applying information technology to support and sustain the monitoring of internal control. Guidance is provided for the design and operation of monitoring activities over existing IT controls; however, customization of the provided approaches, reflecting the specific circumstances of each enterprise, is required.

The main goals/aims of this publication are to:

- Complement and expand on the 2009 COSO *Guidance on Monitoring of Internal Controls*
- Emphasize the monitoring of application and IT general controls
- Discuss the use of automation (tools) for increased efficiency and effectiveness of monitoring processes

This publication will be helpful for executives/senior management, business process owners and IT professionals. 2010, 124 pages. **MIC**

OUTSOURCING IT: A GOVERNANCE GUIDE

Rupert Kendrick

Businesses are increasingly choosing to outsource their IT function. The attraction of outsourcing IT is that it enables a company to obtain an efficient and responsive IT system, while at the same time allowing the company to focus on its core strengths. The current economic climate is also putting companies under increasing pressure to find new ways of cutting costs. However, all too often IT outsourcing projects fail because companies have not applied appropriate governance processes to the project.

The IT function is nearly always a business-critical operation. This means that outsourcing IT will give a supplier control over a function that is vital to the organization's survival and success.

This book offers a guide to the many pitfalls of IT outsourcing. It will provide readers with clear criteria for the application of governance principles to the outsourcing process and, thereby, enable them to implement IT outsourcing so that it supports the overall business goals. 2009, 336 pages **2-ITO**

A PRACTICAL GUIDE TO REDUCING IT COSTS

NEW

Anita Cassidy, Dan Cassidy

Eliminating and driving down costs has long been second nature for many IT organizations. In challenging economic times, even further cutting of IT costs is a requirement for the survival of many organizations. Whether in the midst of an economic downturn or upturn, effective cost management is critical as IT costs can be a significant portion of an organizations overhead cost structure and can even impact an organizations competitive position. *A Practical Guide to Reducing IT Costs* provides a toolkit of innovative ideas to assess and reduce costs in an IT organization. It outlines a compilation of practical advice based on interviews and comments from more than 60 chief information officers and IT leaders, and it includes many other proven ideas that if implemented will successfully reduce IT costs. 2009, 296 pages. **3-JR**

THE SERVICE CATALOG

NEW

Mark O'Loughlin

The Service Catalog means many different things to many different people. However most would agree that a catalog that helps customers and users to quickly identify the services they require clearly adds value. In turn this helps organizations identify key services that support business processes, understand the contribution made by those services and manage them appropriately. This well-constructed book provides practical advice and information that will help organizations to understand how to design and develop a service catalog and understand the role that the service catalog performs within the service portfolio. 2010, 256 pages. **13-VH**

WORLD CLASS IT: WHY BUSINESSES SUCCEED WHEN IT TRIUMPHS

NEW

Peter A. High

Technology are around. It is so pervasive that one may not even recognize when interacting with it. Despite this fact, many companies have yet to leverage information technology as a strategic weapon.

What then are information technology executives to do to raise the prominence of their department? In World Class IT, recognized expert in IT strategy Peter High reveals the essential principles IT executives must follow and the order in which they should follow them whether they are at the helm of a high-performing department or one in need of great improvement. 2009, 192 pages. **87-WWC**

ISACA Bookstore Price List

2011 CISA® EXAM REFERENCE MATERIALS

◆ *To prepare for the* ***December 2011*** *CISA exam, order* ◆

Code	Title		Nonmember	Member
CISA Review Manual 2011*				
CRM-11	English Edition		$135.00	$105.00
CRM-11C	Chinese Simplified Edition		135.00	105.00
CRM-11F	French Edition		135.00	105.00
CRM-11I	Italian Edition		135.00	105.00
CRM-11J	Japanese Edition		135.00	105.00
CRM-11S	Spanish Edition		135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2011*				
QAE-11	English Edition	(900 Questions)	130.00	100.00
QAE-11C	Chinese Simplified Edition	(900 Questions)	130.00	100.00
QAE-11G	German Edition	(900 Questions)	130.00	100.00
QAE-11I	Italian Edition	(900 Questions)	130.00	100.00
QAE-11J	Japanese Edition	(900 Questions)	130.00	100.00
QAE-11S	Spanish Edition	(900 Questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2011 Supplement*				
QAE-11ES	English Edition	(100 Questions)	60.00	40.00
QAE-11CS	Chinese Simplified Edition	(100 Questions)	60.00	40.00
QAE-11FS	French Edition	(100 Questions)	60.00	40.00
QAE-11GS	German Edition	(100 Questions)	60.00	40.00
QAE-11IS	Italian Edition	(100 Questions)	60.00	40.00
QAE-11JS	Japanese Edition	(100 Questions)	60.00	40.00
QAE-11SS	Spanish Edition	(100 Questions)	60.00	40.00
CISA Practice Question Database v11 (1,000 Questions)*				
CDB-11	CD-ROM—English Edition		225.00	185.00
CDB-11W	Download—English Edition (no shipping charges apply to download)		225.00	185.00
CDB-11S	CD-ROM—Spanish Edition		225.00	185.00
CDB-11SW	Download—Spanish Edition (no shipping charges apply to download)		225.00	185.00
CAN*	Candidate's Guide to the CISA Exam and Certification (No charge to paid CISA exam registrants)		15.00	5.00

2011 CISM® EXAM REFERENCE MATERIALS

◆ *To prepare for the* ***December 2011*** *CISM exam, order* ◆

Code	Title		Nonmember	Member
CISM Review Manual 2011*				
CM-11	English Edition		115.00	85.00
CM-11J	Japanese Edition		115.00	85.00
CM-11S	Spanish Edition		115.00	85.00
CISM Review Questions, Answers & Explanations Manual 2011*				
CQA-11	English Edition	(650 Questions)	90.00	70.00
CQA-11J	Japanese Edition	(650 Questions)	90.00	70.00
CQA-11S	Spanish Edition	(650 Questions)	90.00	70.00
CISM Review Questions, Answers & Explanations Manual 2011 Supplement*				
CQA-11ES	English Edition	(100 Questions)	60.00	40.00
CQA-11JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-11SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Practice Question Database v11 (750 Questions)*				
MDB-11	CD-ROM – English Edition		160.00	120.00
MDB-11W	Download – English Edition (no shipping charges apply to download)		160.00	120.00
CGC*	Candidate's Guide to the CISM Exam and Certification (No charge to paid CISM exam registrants)		15.00	5.00

2011 CGEIT EXAM REFERENCE MATERIALS

◆ *To prepare for the* ***December 2011*** *CGEIT exam, order* ◆

Code	Title	Nonmember	Member
CGM-11*	CGEIT Review Manual 2011	115.00	85.00
CGQ-11*	CGEIT Review Questions, Answers & Explanations Manual 2011 English Edition (60 Questions)	60.00	40.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification (No charge to paid CGEIT exam registrants)	15.00	5.00

2011 CRISC EXAM REFERENCE MATERIALS

◆ *To prepare for the* ***December 2011*** *CRISC exam, order* ◆

Code	Title	Nonmember	Member
CRR-11*	CRISC Review Manual 2011	115.00	85.00
CRQ-11*	CRISC Review Questions, Answers & Explanations Manual 2011 (100 Questions)	60.00	40.00
CACR*	Candidate's Guide to the CRISC Exam and Certification (No charge to paid CRISC exam registrants)	15.00	5.00

COBIT®

Code	Title	Nonmember	Member
CB4.1*	COBIT 4.1, Print Format	190.00	75.00
COBIT and Application Controls: A Management Guide			
WCAC*	E-book—PDF format (purchase online only)	55.00	FREE
CAC*	Print format	75.00	35.00
CBX*	COBIT 4.1 Excerpt	5.00	5.00
CPS2*	COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition	110.00	55.00
CBQ2*	COBIT Quickstart, 2nd Edition	110.00	55.00
CBSB2*	COBIT Security Baseline, 2nd Edition	40.00	20.00
	Additional Set (5 each) Reference Cards		
	HRC2 Home Users	3.00	2.00
	PRC2 Professional Users	3.00	2.00
	MRC2 Managers	3.00	2.00
	ERC2 Executives	3.00	2.00
	SRC2 Senior Executives	3.00	2.00
	BRC2 Board of Directors/Trustees	3.00	2.00
COBIT User Guide for Service Managers			
WCUG*	E-book—PDF format (purchase online only)	35.00	FREE
CUG*	Print format	50.00	20.00
CB4A*	IT Assurance Guide: Using COBIT	165.00	55.00
ITG9*	Implementing and Continually Improving IT Governance	115.00	55.00
SDG*	SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach	70.00	30.00
COBIT Online 4.1			
COLB*	**Annual Full Subscription + Benchmarking (purchase online at *www.isaca.org/cobitonline*) ISACA members SAVE 75%**	**400.00**	**~~200.00~~ 50.00**

▶ **Visit *www.isaca.org/cobitonline* for additional information.** ◀

Code	Title	Nonmember	Member
COBIT Mappings			
WCMCMM*	Mapping of CMMI for Development V1.2 With COBIT 4.0	25.00	Free
WCMISO*	Mapping of ISO/IEC 17799: 2005 With COBIT 4.0	25.00	Free
WCMIT3*	Mapping of ITIL V3 With COBIT® 4.1	25.00	Free
WCMNIST*	Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1	25.00	Free
WCMPMB*	Mapping of PMBOK to COBIT 4.0	25.00	Free
WCMSEI*	Mapping of SEI's CMM for Software to COBIT 4.0	25.00	Free
WCMTOG*	Mapping of TOGAF 8.1 With COBIT 4.0	40.00	Free
WCMFF*	Mapping FFIEC with COBIT 4.1	25.00	Free
WCM20000*	Mapping of ISO/IEC 20000 with COBIT 4.1	25.00	Free
WCMCMM2*	Mapping of CMMI for Development V1.2 with COBIT 4.1	25.00	Free

Sets of related COBIT products focusing on your professional needs are available—purchase a focus set and save!
See *www.isaca.org/cobitbooks* for components included in each Focus Set

Meycor CobiT Suite
Comprehensive software for implementing CobiT 4.1 as an IT governance, security or assurance tool. (see *www.isaca.org/cobit* for descriptions and pricing)

See **NON-ENGLISH RESOURCES** for additional COBIT material.

VAL IT™

Code	Title	Nonmember	Member
Enterprise Value: Governance of IT Investments			
VITM*	Getting Started With Value Management	40.00	25.00
VITF2*	The Val IT Framework 2.0	90.00	45.00
VITB2*	The Business Case Guide—Using Val IT 2.0	40.00	25.00
VITAG*	Value Management Guidance for Assurance Professionals—Using Val IT 2.0	40.00	25.00
VITS2*	Complete Set	185.00	105.00

RISK IT AND RISK RELATED TOPICS

Code	Title	Nonmember	Member
78-WRM	The Failure of Risk Management: Why It's Broken and How to Fix It	55.00	45.00
70-WFR	Fraud Risk Assessment: Building a Fraud Audit Program	80.00	70.00
11-CRC8	How to Complete a Risk Assessment in 5 Days or Less	95.00	85.00
84-WRM	Information Technology Risk Management in Enterprise Environments	100.00	90.00
2-HBS	IT Risk: Turning Business Threats Into Competitive Advantage	45.00	35.00
5-PL	Risk Management & Risk Assessment	105.00	95.00
55-WRCS	Risks, Controls, and Security: Concepts and Applications	118.00	108.00
RITF*	The Risk IT Framework	95.00	45.00
RITPG*	The Risk IT Practitioner Guide	115.00	55.00
5-RO	A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance	105.00	95.00

Shaded — New Books * Published by ISACA and ITGI PRICES SUBJECT TO CHANGE

ISACA Bookstore Price List

AUDIT, CONTROL AND SECURITY—ESSENTIALS

Code	Title	Nonmember	Member
48-CRC	Access Control, Security, and Trust: A Logical Approach	100.00	90.00
1-IT8	Accounting Information Systems, 8th Edition	233.00	223.00
70-WAS	Accounting Information Systems: Controls and Processes	169.00	159.00
6-PAW	Applied Security Visualization	65.00	55.00
45-WAP	Audit Planning: A Risk-Based Approach	80.00	70.00
6-PL	Auditing IT Infrastructures	105.00	95.00
53-WAG	Auditor's Guide to Information Systems Auditing	115.00	105.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00
43-CRC	Building an Effective Information Security Policy Architecture	90.00	80.00
31-CRC	Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI	140.00	130.00
79-WCAF	Computer Aided Fraud Prevention and Detection: A Step by Step Guide	70.00	60.00
4-IGI	Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions	110.00	100.00
1-JBCS	Computer Security: Protecting Digital Resources	93.00	83.00
30-WCC	Core Concepts of Information Technology Auditing	99.00	89.00
50-WPM5	Effective Project Management: Traditional, Agile, Extreme, 5th Edition	60.00	50.00
	Enterprisewide Identity Management		
WIM*	E-book—PDF Format (purchase online only)	20.00	10.00
PIM*	Print Format	35.00	25.00
1-ABES	Enterprise Security for the Executive: Setting the Tone from the Top	45.00	35.00
71-WCF	Essentials of Corporate Fraud	55.00	45.00
60-WESO	Essentials of Sarbanes-Oxley	45.00	35.00
82-WACL	Fraud Analysis Techniques Using ACL	210.00	200.00
62-WFC	Fraud Casebook: Lessons from the Bad Side of Business	80.00	70.00
10-EL	GFI Network Security and PCI Compliance Power Tools	73.00	63.00
36-CRC	How to Achieve 27001 Certification: An Example of Applied Compliance Management	100.00	90.00
2-W404	How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control, 3rd Edition	95.00	85.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	105.00	95.00
9-CRC	Information Security Architecture: An Integrated Approach to Security in the Organization, 2nd Edition	100.00	90.00
28-CRC	Information Security: Design, Implementation, Measurement and Compliance	110.00	100.00
83-WIS	Information Storage and Management: Storing, Managing, and Protecting Digital Information	70.00	60.00
4-CRC3	Information Technology Control and Audit, 3rd Edition	100.00	90.00
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
WITAF*	ITAF: A Professional Practices Framework for IT Assurance e-book—PDF (purchase online only)	45.00	FREE
8-PL	IT Auditing: The Process	105.00	95.00
15-MIT2	IT Auditing Using Controls to Protect Information Assets, 2nd Edition	80.00	70.00
	IT Control Objectives for Basel II		
WITCOB*	E-book—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
PSOX*	IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition	7.00	7.00
9-SYN	The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments	83.00	73.00
22-MSM	IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data	60.00	50.00
6-ITSOC	IT Strategic and Operational Controls	70.00	60.00
1-IIA	A New Auditor's Guide to Planning, Performing, and Presenting IT Audits	80.00	70.00
5-ART	Outsourcing Information Security	103.00	93.00
7-SYN9	PCI Compliance, Second Edition	70.00	60.00
1-RIA	Practical IT Auditing with current Supplement	420.00	410.00
2-SAPP	SAP Security and Risk Management, 2nd Edition	80.00	70.00
75-WSO	The Sarbanes-Oxley Section 404 Implementation Toolkit: Practice Aids for Managers and Auditors, 2nd Edition	100.00	90.00
1-IGI	Securing the Information Infrastructure	110.00	100.00
5-PSM	Security Metrics: Replacing Fear, Uncertainty, and Doubt	70.00	60.00
2-WG	Standard for Auditing Computer Applications	509.00	499.00
2-BAY*	Stepping Through the InfoSec Program	45.00	35.00
1-BAY*	Stepping Through the IS Audit, 2nd Edition	45.00	35.00

AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS

Code	Title	Nonmember	Member
18-MAO	Applied Oracle Security: Developing Secure Database and Middleware Environments	70.00	60.00
4-DC	Audit Guidelines for DB2	80.00	70.00
1-SAPP	COBIT and the Sarbanes-Oxley Act	45.00	35.00
88-WFA	Fraud Auditing and Forensic Accounting, 4th Edition	85.00	75.00
10-ART	Identity Management: Concepts, Technologies, and Systems	110.00	100.00
	Linux: Security, Audit and Control Features		
WLIN*	E-book—PDF Format (purchase online only)	30.00	15.00
PLIN*	Print Format	50.00	35.00
	Managing Risk in Wireless Environment: Security, Audit and Control Issues		
WW*	E-book—PDF Format (purchase online only)	40.00	20.00
PW*	Print Format	50.00	35.00
1-IPG	Oracle Privacy Security Auditing	70.00	60.00
OS390*	OS/390-z/OS Security, Audit and Control Features	70.00	55.00
29-ST4	A Practical Guide to IBM i and i5/OS Security and Compliance	89.00	79.00
1-MPPI	Protecting Industrial Control Systems from Electronic Threats	100.00	90.00
ODB9*	Security, Audit and Control Features Oracle® Database, 3rd Edition	55.00	40.00
ISOA3*	Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition	75.00	60.00
ISPS*	Security, Audit and Control Features PeopleSoft®, 2nd Edition	70.00	55.00
ISAP3*	Security, Audit and Control Features SAP® ERP, 3rd Edition	75.00	60.00
3-EL	Wireless Operational Security	95.00	85.00

NON-ENGLISH RESOURCES

2-TCA	Administración de la Seguridad de Información	55.00	45.00
3-RAMA	Auditoría de Tecnologías y Sistemas de Información	70.00	60.00

CISA Examination Reference Material
Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the December 2011 CISA exam—see page S1

CISM Examination Reference Material
Study aids available in Japanese and Spanish for the December 2011 CISM exam—see page S1

COBIT 3rd Edition, available at the following web site
Korean Edition—*www.isaca.or.kr*

COBIT 4.0 Edition, available at the following web sites
German Edition—*www.isaca.at*
Italian Edition—*www.aiea.it*

COBIT 4.1 Edition, available at the following web site
French Edition—*www.afai.fr*
Japanese Edition—*www.isaca.gr.jp*
Hungarian Edition—*www.isaca.hu*
Portuguese Edition—*www.isaca.org/downloads*
Russian Edition—*www.isaca-russia.ru*
Spanish Edition—*www.isaca.org/downloads*

1-AOCF	Computación Forense: Descubriendo los Rastros Informáticos	42.00	32.00

Meycor COBIT Suite
Meycor COBIT es un software completo e integrado para la implementación de COBIT como una herramienta para el Buen Gobierno de la TI, Seguridad de la TI o Aseguramiento de la TI según COBIT 4.1. (see *www.isaca.org/nonenglishbooks* para descripción y precios)

1-TCA	Principios de Auditoría y Control de Sistemas de Información	40.00	30.00
ISOAJ*	Security, Audit and Control Features Oracle E-Business Suite: A Technical and Risk Management Reference Guide—(Japanese Version)	70.00	55.00
ISAPJ*	Security, Audit and Control Features SAP R/3: A Technical and Risk Management Reference Guide—(Japanese Version)	70.00	55.00

INTERNET AND RELATED SECURITY TOPICS

19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
1-NBS	The Big Switch: Rewiring the World, from Edison to Google	27.00	17.00
45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
10-MOC	The Complete Reference Network Security	73.00	63.00
9-EL	Computer and Information Security Handbook	130.00	120.00
	Cybercrime: Incident Response and Digital Forensics		
WCC*	E-book—PDF Format (purchase online only)	45.00	25.00
PCC*	Print Format	55.00	40.00
11-EL	Cyber Attacks: Protecting National Infrastructure	70.00	60.00
1-CAP	Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 2nd Edition	47.00	37.00
2-SCC	Cybercrimes: A Multidisciplinary Analysis	199.00	189.00
34-CRC	Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition	90.00	80.00
4-MGH3	Gray Hat Hacking: The Ethical Hakers Handbook, 3rd Edition	70.00	60.00
1-MHF	Hacking Exposed Computer Forensics Secrets and Solutions, 2nd Edition	60.00	50.00
2-MCG6	Hacking Exposed: Network Security Secrets & Solutions, 6th Edition	60.00	50.00
23-MHE	Hacking Exposed Web Applications, 3rd Edition	60.00	50.00
17-MHE2	Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 2nd Edition	60.00	50.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00

Shaded — New Books * Published by ISACA and ITGI PRICES SUBJECT TO CHANGE

ISACA Bookstore Price List

Code	Title	Nonmember	Member
59-WNS	Network Security Fundamentals	80.00	70.00
1-GL	NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning	60.00	50.00
1-WCNR	No Root for You: A Series of Tutorials, Rants and Raves, and Other Random Nuances Therein	33.00	23.00
56-WPC	Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft	105.00	95.00
1-HA	Scrappy Information Security: The Easy Way to Keep the Cyber Wolves at Bay	30.00	20.00
30-CRC	Securing Converged IP Networks	100.00	90.00
24-MSIEM	Security Information and Event Management (SIEM) Implementation	75.00	65.00
1-OSM	Security Monitoring	55.00	45.00
2-JBSF	System Forensics, Investigation, and Response	100.00	90 .00
6-EL	XSS Exploits—Cross Site Scripting Attacks and Defense	73.00	63.00

IT GOVERNANCE AND BUSINESS MANAGEMENT

3-PAGE	7 Steps to Better Written Policies and Procedures	30.00	20.00
2-PAGE	Achieving 100% Compliance of Policies and Protection	50.00	40.00
8-EL	Architecture and Patterns for IT Service Management, Resource Planning, and Governance: Making Shoes for the Cobbler's Children	57.00	47.00
61-WBSC	Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 2nd Edition	60.00	50.00
4-PAGE	Best Practices in Policies and Procedures	36.00	26.00
1-ITG*	Board Briefing on IT Governance, 2nd Edition	7.00	7.00
66-WCP	Building a World-Class Compliance Program: Best Practices and Strategies for Success	55.00	45.00
6-SYN	Business Continuity and Disaster Recovery Planning for IT Professionals	70.00	60.00
BMIS*	The Business Model for Information Security	60.00	45.00
41-CRC	Business Resumption Planning, 2nd Edition	108.00	98.00
39-CRC	The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results	86.00	76.00
54-WCIO2	CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition	75.00	65.00
74-WCM	Corporate Management, Governance, and Ethics Best Practices	80.00	70.00
WCCS*	Creating a Culture of Security (e-book)	50.00	FREE
32-CRC	Crisis Management Planning and Execution	90.00	80.00
1-WBC	The Definitive Handbook of Business Continuity Management, 2nd Edition	85.00	75.00
37-CRC	Digital Privacy: Theory, Technologies, and Practices	90.00	80.00
2-IGI	Emerging Topics and Technologies in Information Systems	205.00	195.00
89-WEG	Empowering Green Initiatives with IT: A Strategy and Implementation Guide	60.00	50.00
9-ART	Enterprise Information Security and Privacy	109.00	99.00
1-CMP	Enterprise Security Architecture: A Business-Driven Approach	97.00	87.00
23-WIT	The Executive's Guide to Information Technology, 2nd Edition	105.00	95.00
10-VH	Foundations of IT Service Management Based on ITIL® V3	66.00	56.00
3-VH	Frameworks for IT Management	66.00	56.00
85-WF101	Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition	60.00	50.00
64-WGRC	Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices	165.00	155.00
42-CRC	The Green and Virtual Data Center	90.00	80.00
7-ITGR	Green IT in Practice, 2nd Edition	60.00	50.00
20-MHE	Hacking Exposed Malware and Rootkits: Malware & Rootkits Secrets & Solutions	60.00	50.00
67-WHF	Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation	60.00	50.00
WGOALS*	Identifying and Aligning Business Goals and IT Goals (E-book—PDF purchase online only)	35.00	20.00
4-ID	Implementing Information Technology Governance: Models, Practices and Cases	110.00	100.00
7-VH	Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management	66.00	56.00
46-CRC	Implementing the Project Management Balanced Scorecard	90.00	80.00
2-ITG*	Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition	7.00	7.00
	Information Security Governance: Guidance for Information Security Managers		
3-ITG*	Information Security Governance: Guidance for Information Security Managers	50.00	25.00
W3ITG*	E-book—PDF Format (purchase online only)	45.00	FREE
WSH*	Information Security Harmonisation: Classification of Global Guidance (E-book—PDF format purchase online only)	40.00	FREE
1-BS	Information Security Policies Made Easy, Version 11	805.00	795.00
2-PS	Information Security Roles & Responsibilities Made Easy, Version 2	505.00	495.00
3-IGI	Information Technology Governance and Service Management: Frameworks and Adaptations	205.00	195.00
80-WITM8	Information Technology for Management: Improving Strategic and Operational Performance, 8th Edition	201.00	191.00
81-WIC	Internal Controls Policies and Procedures	90.00	80.00
5-VH	ISO/IEC 20000: A Pocket Guide	33.00	23.00
12-VH	IT Financial Management	66.00	56.00
3-ITGD	IT Governance: Guidelines for Directors	90.00	80.00
4-ITIG	IT Governance: A Pocket Guide	26.00	16.00
5-AS11	IT Governance: Policies & Procedures, 2011 Edition	235.00	225.00
WGPM*	IT Governance and Process Maturity (E-Book—purchase online only)	30.00	FREE
5-ITOC	IT Outsourcing Contracts: A Legal and Practical Guide	41.00	31.00
11-VH	IT Outsourcing: Part 1 Contracting the Partner	42.00	32.00
25-MIPM	IT Project Management: On Track from Start to Finish, 3rd Edition	60.00	50.00
47-CRC	IT Service Management: Implementation and Operation	80.00	70.00
40-CRC	Leading IT Projects: The IT Manager's Guide	96.00	86.00
49-WMG	Manager's Guide to Compliance: Best Practices and Case Studies	80.00	70.00
	Managing Enterprise Information Integrity: Security, Control and Audit Issues		
WME*	E-book—PDF Format (purchase online only)	45.00	25.00
PME*	Print Format	55.00	40.00
9-VH	MOF—Microsoft Operations Framework V4.0: A Pocket Guide	33.00	23.00
MIC*	Monitoring Internal Control Systems and IT	70.00	55.00
2-ITO	Outsourcing IT: A Governance Guide	82.00	72.00
3-JR	A Practical Guide to Reducing IT Costs	60.00	50.00
6-RO	Principles and Practice of Business Continuity: Tools and Techniques	109.00	99.00
1-IS	The Privacy Management Toolkit	505.00	495.00
1-HBS	Reinventing Project Management: The Diamond Approach to Successful Growth and Innovation	45.00	35.00
5-SYN	Sarbanes-Oxley IT Compliance Using Open Source Tools, 2nd Edition	73.00	63.00
	Security Awareness: Best Practices to Secure Your Enterprise		
WSA*	E-book—PDF Format (purchase online only)	35.00	20.00
PSA*	Print Format	50.00	35.00
13-VH	The Service Catalog	66.00	56.00
58-WSOA	Service Oriented Architecture: A Planning and Implementation Guide for Business and Technology	70.00	60.00
73-WSOA	Service Oriented Architecture Field Guide for Executives	60.00	50.00
77-WTS	Technology Scorecards: Aligning IT Investments with With Business Performance	60.00	50.00
4-ITG*	Unlocking Value: An Executive Primer on the Critical Role of IT Governance	7.00	7.00
2-ITPI	Visible OPS Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps	32.00	22.00
44-CRC	Vulnerability Management	90.00	80.00
1-EA	Winning as a CISO	30.00	20.00
87-WWC	World Class IT: Why Businesses Succeed When IT Triumphs	48.00	38.00

Shaded — New Books * Published by ISACA and ITGI PRICES SUBJECT TO CHANGE

FOUR EASY WAYS TO PLACE AN ORDER:

Online
Order online at
www.isaca.org/bookstore

BankWires:
Send electronic payments in US dollars to:
Bank of America, ABA #0260-0959-3
ISACA Account #22-71578
S.W.I.F.T code BOFAUS3N

Mail
Mail completed form with payment:
ISACA/ITGI
1055 Paysphere Circle
Chicago, IL 60674-1055 USA

Fax
Fax completed order form with credit card number and expiration date to +1.847.253.1443

RETURN POLICY

All purchases are final. No refunds or exchanges.

PUBLICATION QUANTITY DISCOUNTS

Academic and bulk discounts are available on books published by the ISACA and IT Governance Institute. Please call +1.847.660.5501 or +1.847.660.5578 for pricing information.

Phone
+1.847.660.5650
Monday-Friday, 8:00 am-5:00 pm Central Time (Chicago, Illinois, USA) Personal service—please have credit card number available. We will confirm availability and expected delivery date.

ISACA® Customer Order Form

Trust in, and value from, information systems

OFFICE USE ONLY

Vol. 4 -11

PLEASE NOTE: READ PAYMENT TERMS AND SHIPPING INFORMATION BELOW. ALL ORDERS MUST BE PREPAID.

U.S. Federal I.D. No. 23-7067291

Please return to: ISACA, 1055 Paysphere Circle, Chicago, IL 60674, USA
Phone: +1.847.660.5650 Fax: +1.847.253.1443 E-mail: *bookstore@isaca.org*

Your contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. To learn more, please visit *www.isaca.org* and read our Privacy Policy.

Customer Information

Name _____
FIRST MIDDLE LAST/FAMILY

ISACA Member: ☐ No ☐ Yes Member Number _____

Company Name _____

Address: ☐ Home ☐ Company

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

Fax Number ( ) _____

E-mail Address _____

Shipping Information (If different from customer information)

If shipping to a PO Box, please include street address to ensure proper delivery.

Name _____
FIRST MIDDLE LAST/FAMILY

Company Name _____
(IF PART OF SHIPPING ADDRESS)

Address: _____

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

E-mail Address _____

Code	Title/Item	Quantity	Unit Price	Total

Thank you for ordering from ISACA. **All purchases are final.**

Subtotal	
Sales Tax: Add sales tax if shipping to: Louisiana (LA), Oklahoma (OK)—4%	
Wisconsin (WI)—5%	
Florida (FL), Minnesota (MN), Pennsylvania (PA), South Carolina (SC), Texas (TX), Washington (WA)—6%	
New Jersey (NJ), Tennessee (TN)—7%	
California (CA)—8%	
Illinois (IL)—9%	
For all orders please include shipping and handling charge—see chart below.	
TOTAL	

Payment Information—Prepayment Required

☐ Payment enclosed. Check payable to "ISACA" in US dollars, drawn on US bank.

☐ Bank wire transfer in US dollars. Date of transfer _____

☐ Charge to ☐ Visa ☐ MasterCard ☐ American Express ☐ Diners Club

Credit Card # _____

Exp. Date _____

Print Cardholder Name _____

Signature of Cardholder _____

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

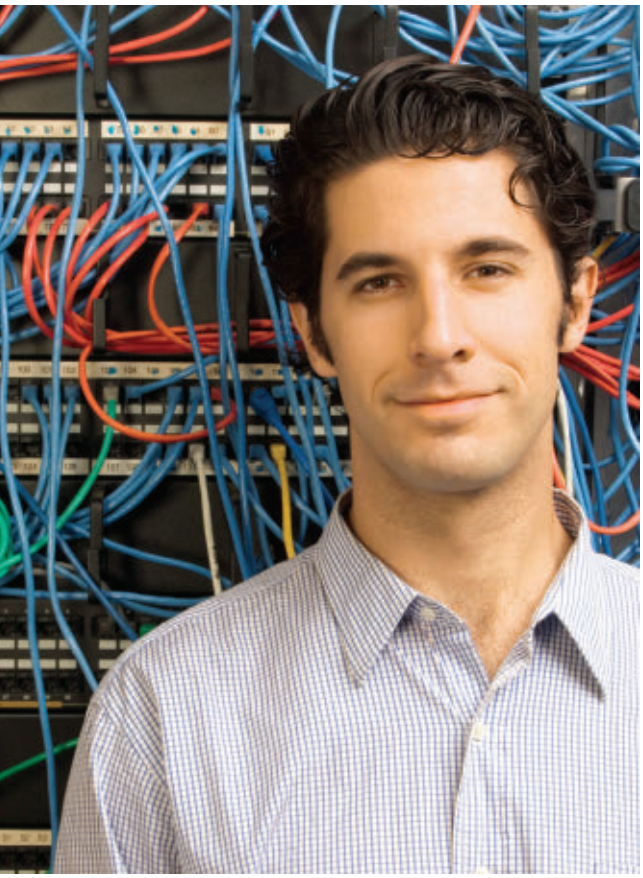
For Orders Totaling	Outside US	Within US
Up to US $30.00	US $10.00	US $5.00
US $30.01 to US $50.00	US $15.00	US $7.00
US $50.01 to US $80.00	US $20.00	US $8.00
US $80.01 to US $150.00	US $26.00	US $10.00
Over US $150.00	17% of Total	10% of Total

No shipping charges apply to *Meycor COBIT.*
No shipping charges apply to CISA Practice Question Database v11—download.
No shipping charges apply to CISM Practice Question Database v11—download.

Shipping details *www.isaca.org/shipping*
International customers are solely responsible for paying all custom duties, service charges, and taxes levied by their country.

All purchases are final. **Pricing, shipping and handling, and tax are subject to change without notice.**

KEEP YOUR CAREER ON TRACK



At Regis University, we believe that information assurance professionals should have the knowledge to maximize the use of data within an organization as well as protect it. As a result, our Information Assurance programs are grounded in security but also focus on delivering the requisite combination of IT and business acumen **— creating a link between the server room and the boardroom.**

Available programs – online or on-campus:

MASTER OF SCIENCE IN INFORMATION ASSURANCE

- General track
- Specialization in Cyber Security
- Specialization in Information Assurance Policy Management

Regis University is designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency. The curriculum is modeled on the guidelines and recommendations provided by the Committee on National Security Systems (CNSS) 4000 training standards, the (ISC)^2 International Information Systems Security Certification Consortium Ten Domains of Knowledge, and ISACA.

The program can be taken on campus or completely online

REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

RegisDegrees.com/ISACA | 1-877-820-0581